Telecommunication
Development Bureau (BDT)

Ref. BDT/IEE/CYB/DM-045

15 de Mayo del 2015

- Administraciones de los Países Miembros de la UIT de la región AMS
- Miembros de la UIT-D de la región AMS
- Organizaciones Regionales e Internacionales

Asunto: **Foro de Ciberseguridad y Tercer taller ejercicio práctico de aprendizaje aplicado para equipos de respuesta ante emergencias cibernéticas para la región de América, Bogotá, Colombia, 3-6 Agosto 2015**

Estimado(a) Sr./Sra.,

Por medio de la presente, reciba la invitación al **Foro de Ciberseguridad y Tercer taller ejercicio práctico de aprendizaje aplicado para equipos de respuesta ante emergencias cibernéticas para la región de América** (**ALERT**, por sus siglas en inglés).

El evento se realizara del 3 al 6 de Agosto del 2015 en Bogotá, Colombia, contando con la amable invitación del Ministerio de Tecnologías de la Información y las Comunicaciones y la Cámara Colombiana de Informática y Telecomunicaciones (CCIT). Contamos también con el apoyo y colaboración de La Universidad de los Andes, en cuyas instalaciones se realizará el evento. El Anexo contiene información detallada del ejercicio práctico.

El Foro comprende varias sesiones sobre el panorama y perspectivas regionales, protección de la niñez en la utilización de las TIC, el punto de vista del sector público, del sector privado, de la academia, se contará con la participación de entidades regionales, expertos de varias partes del mundo, varias charlas técnicas y adicionalmente el tercer taller ejercicio práctico de aprendizaje aplicado para equipos de respuesta ante emergencias cibernéticas.

Le solicitamos la participación de una delegación de al menos dos profesionales en Ciberseguridad de su Equipo Nacional de Respuesta Ante Incidentes Computacionales (CIRT, por sus siglas en inglés). Por favor considere que su delegación incluya un experto en Ciberseguridad con la atribución de toma de decisiones, ya que durante el evento se discutirá sobre el apoyo regional, colaboración y el establecimiento de un acuerdo de cooperación y trabajo en conjunto entre los CIRTs de la región.

El objetivo de este foro y del tercer taller ejercicio práctico es fomentar cada vez más la interrelación entre los CIRT de la región, capacitar y ofrecer el escenario adecuado para analizar casos reales de ataques cibernéticos, incentivar el trabajo conjunto y así mejorar las capacidades de respuesta ante incidentes de los equipos participantes. Se buscará el llegar a un acuerdo entre los CIRT participantes para asegurar esfuerzos colectivos regionales continuos contra las amenazas cibernéticas.

Para participar en el evento, por favor regístrese en línea **hasta el 24 de Julio del 2015** utilizando el siguiente enlace: http://www.itu.int/go/regitud. Por favor considere, en el caso fuere necesario, el procedimiento de solicitud de visa para ingresar a Colombia. La aprobación de la visa puede tomar cierto tiempo y posiblemente

requiera de una carta de invitación del Ministerio de Tecnologías de la Información y las Comunicaciones para presentarla en la correspondiente embajada/consulado de Colombia en su País.

Información adicional sobre el evento como la agenda, información práctica, etc. La encontrará disponible en la página web del evento:

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

El Sr. Pablo Palacios (Oficina de la UIT en Santiago, Chile), E-mail: pablo.palacios@itu.int, Tel:+ +562 2632 6134/ 562 2632 6147 queda a su disposición en el caso de requerir mayor información.

Atentamente,

Brahima Sanou
Director

Anexo: Información del ejercicio ALERT.

ANEXO

Cyber Drill

Table of Contents

Ejecución del Taller práctico

El taller práctico está basado en un escenario ficticio para estimar la capacidad de manejo de incidentes de parte del CERT. El ejercicio está estructurado sobre un escenario que incluye varios incidentes que presentan los más comunes tipos de ataques cibernéticos. Los detalles de los ataques cibernéticos serán enviados por el grupo de expertos de la ITU, los cuales serán reconocidos como "organizador" para los participantes en los correos electrónicos. Los participantes deben desarrollar su investigación/análisis respectivo del incidente y presentar una solución para mitigar el ataque. El participante debe presentar la solución a la dirección de correo electrónico del organizador en el formato del respectivo reporte consultivo.

Pasos

1. El escenario inicia cuando los participantes reciben el correo electrónico de parte del **organizador** quien presenta el incidente cibernético
2. El correo electrónico contiene:
    a. El escenario
    b. El formato del reporte consultivo
3. Los **participantes** del ejercicio práctico necesitan realizar un análisis del incidente cibernético y presentar una solución para mitigarlo
4. Los observadores del ejercicio práctico pueden asistir a los participantes principales para realizar el correspondiente análisis
5. Los **participantes** deben presentar la solución o las recomendaciones para mitigar el ataque cibernético al organizador por correo electrónico utilizando el formato del reporte consultivo
6. **El organizador** enviara a los participantes un respuesta confirmando la recepción del correo electrónico con la respectiva solución

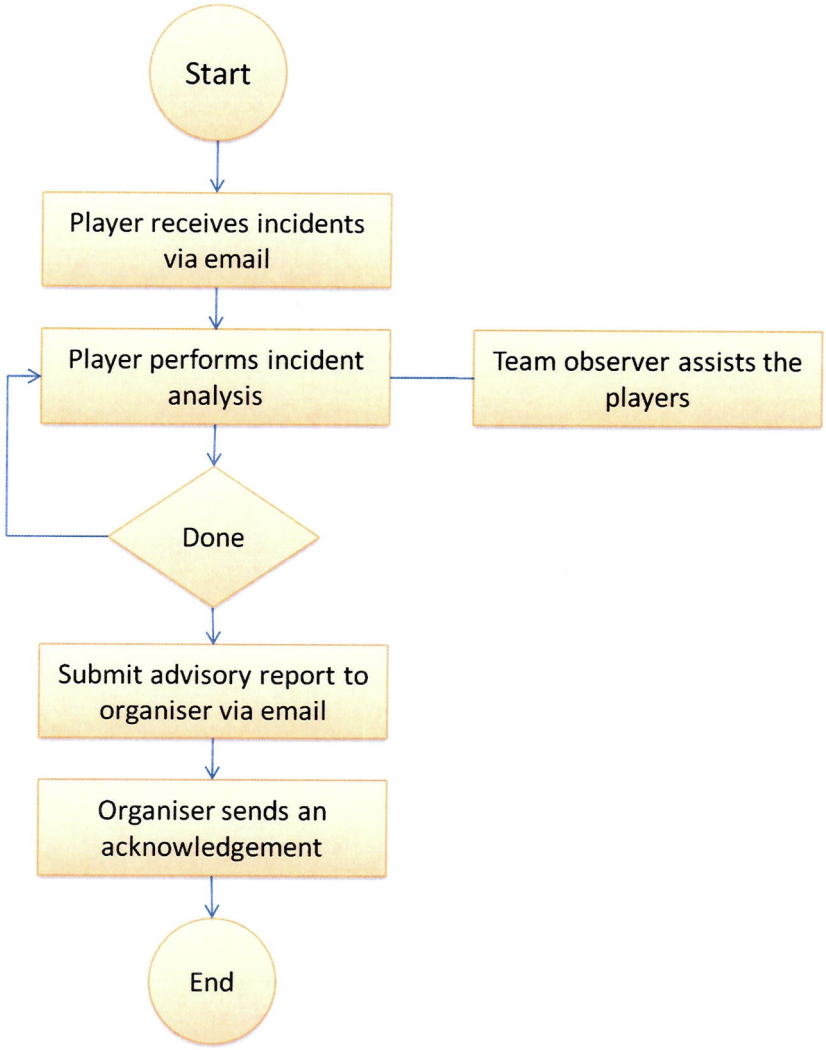

Figura 1: Flujo grama de ejecución del ejercicio práctico

Ejercicio Práctico – Que hacer y Que no hacer

Que Hacer

- Los participantes pueden usar sus propias herramientas de software;
- Los participantes pueden utilizar Google o cualquier otra página web de referencia para buscar información;
- Los participantes pueden comunicarse con otros equipos participantes por medio de IRC;
- Los participantes pueden buscar asistencia del administrador por medio de IRC;

Que no Hacer

- No está permitida ninguna actividad maliciosa que pueda afectar la red como Scanning, Sniffing, DOS o cualquier otro intento de ataque a la infraestructura del ejercicio práctico (por ejemplo al servidor IRC, al servidor web, etc.);
- No está permitido el mal uso de Internet;

Comunicaciones

Servidor de correo electrónico	Toda comunicación formal entre el organizador y los participantes se realizará a través del servidor de correo electrónico
Servidor IRC	Será utilizado para: • Comunicación informal entre el organizador, los participantes y los observadores • Como canal para que los participantes realicen preguntas o soliciten consejos sobre el escenario de ataque • Para notificaciones rápidas de parte del organizador • Para colaborar con otros equipos CIRT participantes, así como con el organizador
Servidor DNS	Servidor local DNS

Configuración física para el ejercicio practico

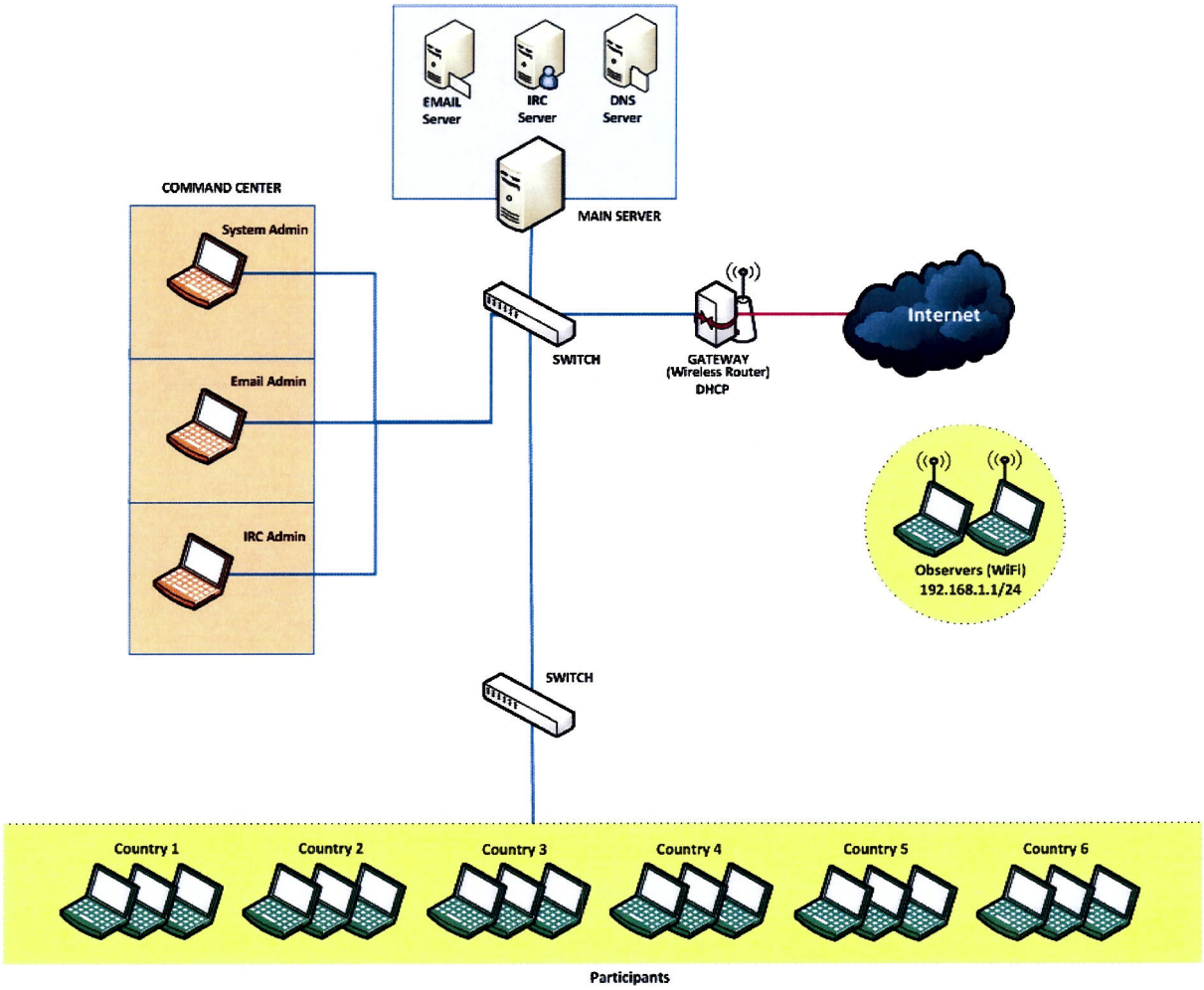

Figura 2: Configuración física para ejercicio práctico

Participantes – Roles & Responsabilidades

Participantes	• Analizar el escenario del incidente y entregar al organizador la solución y/o las recomendaciones para mitigarlo utilizando el formato del reporte consultivo • Áreas de conocimiento que deben tener los participantes: o Conocimiento de Linux OS y Línea de Comandos o Conocimiento de Windows OS y Sistema de Archivos o Paquete de herramientas de sniffing o Herramientas de análisis de mobile malware o Herramientas de análisis de Log o Conocimiento básico de codificación y decodificación de texto o Conocimiento básico de Seguridad de Redes o Buen conocimiento de técnicas de ciber ataques
Observador	• Observar y asistir durante el ejercicio práctico a los participantes de su grupo

Organizador – Roles & Responsabilidades

Director del Ejercicio Practico	• Coordinación global con los expertos y los participantes de los diferentes países
Facilitador del Ejercicio Practico	• Administrar el ejercicio práctico coordinando las actividades de los expertos y los países participantes • Asistir a los participantes durante el ejercicio practico • Guiar los grupos a través de los escenarios durante el desarrollo del ejercicio practico • Presentar el resumen del ejercicio práctico a los participantes
Administrador del Ejercicio Practico	• Administración y coordinación del ejercicio practico • Asistir a los participantes durante el ejercicio practico
Administrador del Sistema	• Responsable de los servidores y máquinas virtuales para el ejercicio practico • Administrar el desarrollo del ejercicio práctico para todos los participantes • Manejar las actividades dentro de la infraestructura del ejercicio práctico provisto para los participantes • Asistir a los participantes durante el ejercicio practico
Administracion del servidor de correo electrónico	• Responsable por las comunicaciones de correo electrónico para el ejercicio practico • Ayudar en la coordinación de las actividades de los participantes durante el ejercicio práctico a través de correo electrónico • Introducir elementos adicionales al escenario a través de correo electrónico durante el ejercicio practico • Recapitular contribuciones para posterior resumen y análisis del ejercicio practico • Asistir a los participantes durante el ejercicio practico
Administrador del servidor IRC	• Responsable por las comunicaciones a través de canales de IRC • Comunicar y coordinar las actividades de los participantes para alcanzar conclusiones en los escenarios presentados • Administrar escenarios presentados durante el ejercicio practico • Recapitular contribuciones para posterior resumen y análisis del ejercicio practico • Asistir a los participantes durante el ejercicio practico
Soporte tecnico e IT	• Desarrollar y apoyar con la infraestructura IT que implica implementar y desmantelar el hardware, software y los sistemas operativos • Proveer solución de problemas, seguridades y administración de todas las redes de dispositivos, servidores e infraestructura • Asistir a los participantes durante el ejercicio practico

Pre-Requisitos para los participantes

Los participantes deben traer sus propios computadores portátiles para el ejercicio práctico.

Requisitos de Hardware/Software:

- Computador portátil con mínimo 2GB RAM y conexión inalámbrica;
- Sistema operativo Windows XP o versión más actual;
- Ultima versión de explorador de Internet (IE, Firefox o Chrome) que contenga instalado flash y Java;
- Procesador de palabras (MS Word, OpenOffice, AbiWord, etc.);

Es recomendado que los participantes tengan conocimientos en las siguientes áreas:

- Recompilation de Information;
- Análisis de Registros (Logs);
- Análisis de Paquetes;

Los participantes deben tener familiaridad con las siguientes herramientas:

- Wireshark;
- Línea de commandos UNIX ;

Cada equipo participante debe tener como mínimo tres (3) personas y como máximo (4) cuatro personas para participar en el ejercicio práctico.

Actividades Posteriores

Todos los equipos participantes deben entregar una evaluación del ejercicio práctico al organizador. La evaluación será entregada por el organizador.

El organizador consolidara las evaluaciones y preparara el respectivo reporte.