UIT-IMPACT ALERT

Ejercicio practico

Table of Contents

Antecedentes

La Unión Internacional de Telecomunicaciones (UIT) y la Colaboración Internacional Multilateral Contra Amenazas Cibernéticas (IMPACT, por sus siglas en inglés) están organizando colectivamente un taller Ciberdrill denominado “ITU-IMPACT ALERT” (Aprendizaje Aplicado para Equipos de Respuesta ante Emergencias Cibernéticas) el cual tendrá una duración de un día y medio. En el año 2008, IMPACT firmó un Memorando de Entendimiento con la UIT para operar su Agenda Global en Ciberseguridad (GCA, por sus siglas en ingles). Parte esencial de la agenda es el buscar cooperación internacional a través de programas específicos como ejercicios coordinados de Ciberdrill entre países.

El propósito del ejercicio práctico de simulación es el de mejorar la comunicación y las capacidades de respuesta de los equipos participantes. Adicionalmente se busca mantener y fortalecer la cooperación Nacional e Internacional entre países para asegurar esfuerzos colectivos contra amenazas cibernéticas.

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 ITU-IMPACT, los cuales serán reconocidos como “organizador” para los participantes en el formato de 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

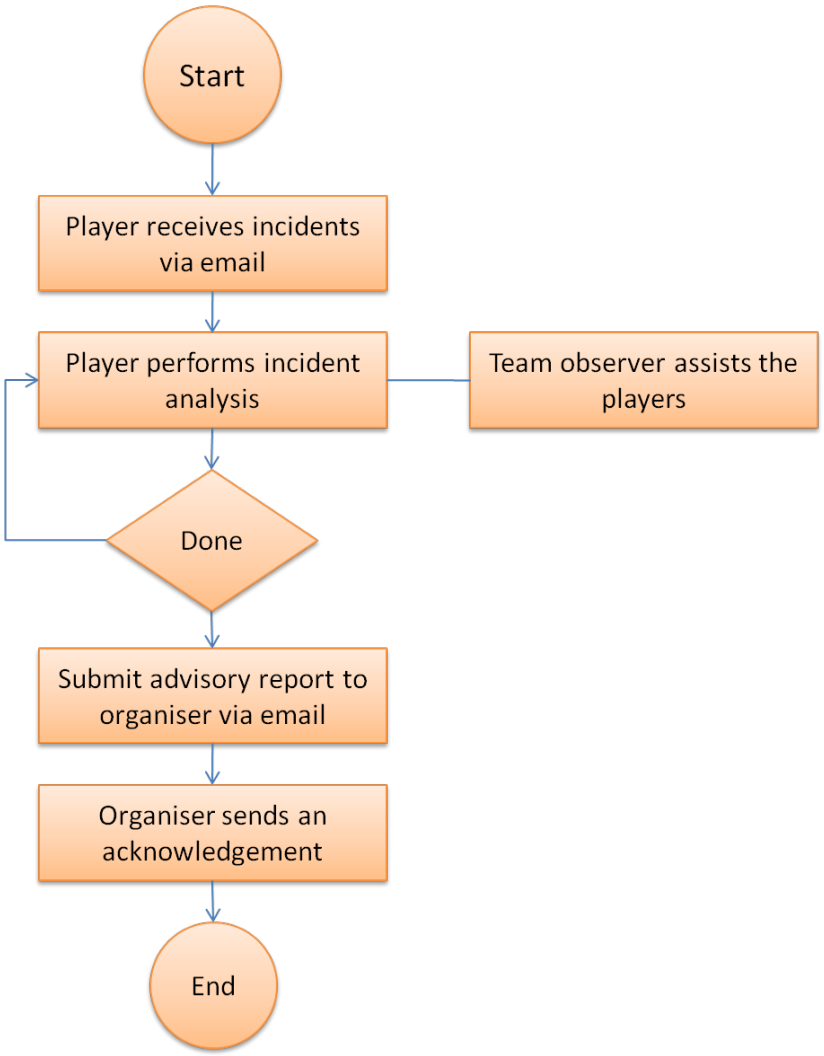

Figura 1: Flujo grama de ejecución del ejercicio práctico

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)
- No está permitido el mal uso de Internet

Comunicaciones

Servidor de correo electronico	Toda comunicación formal entre el organizador y los participantes se realizara a través del servidor de correo electrónico
Servidor IRC	Sera 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 para el dominio IMPACT-ALERT.NET

Configuración física para el ejercicio practico

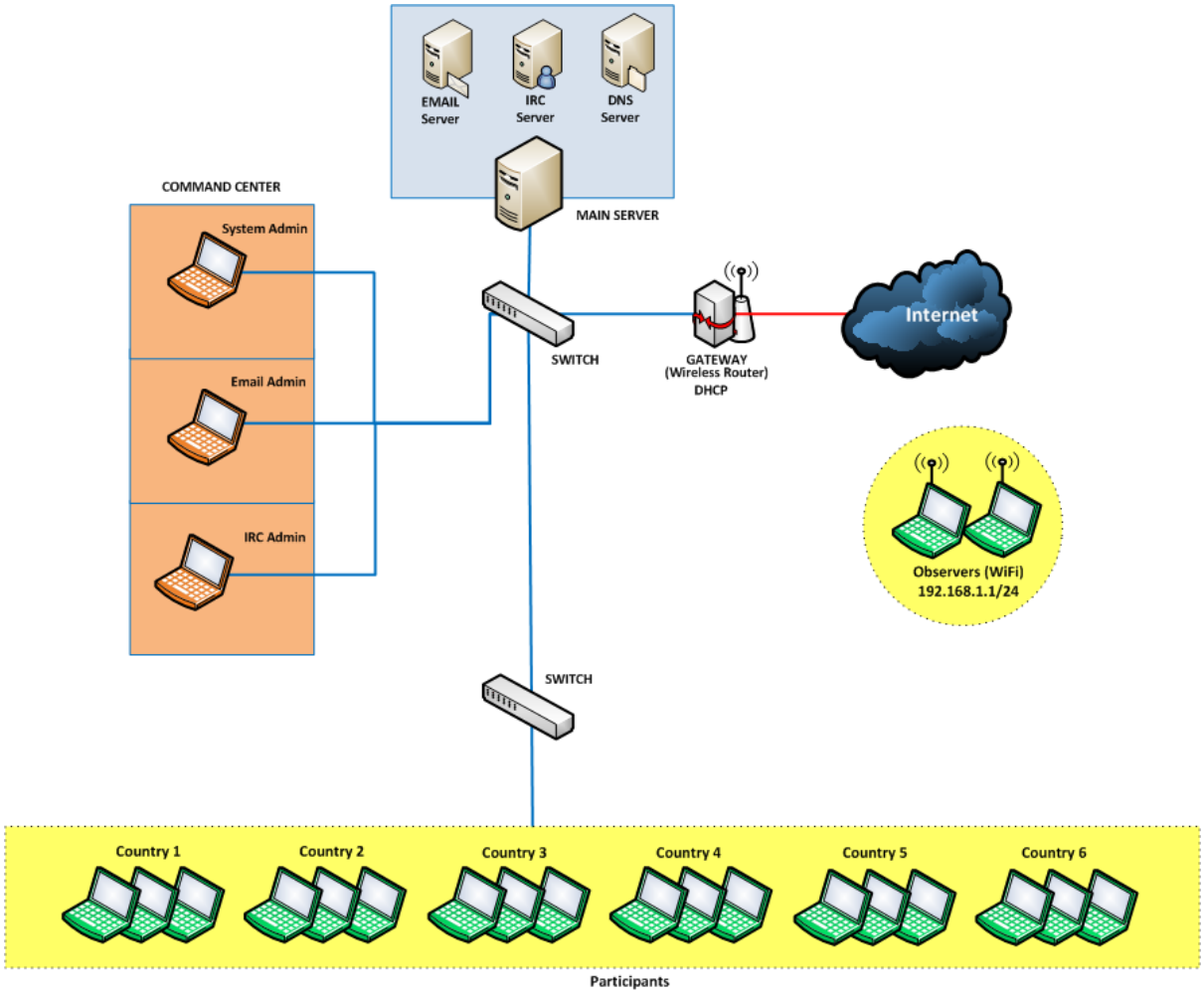

Figura 2: Configuración física para ejercicio práctico

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 consultativo.
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 electronico	• 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
IRC Administrator	• Responsable por las comunicaciones a través de canales de IRC para el ejercicio practico • 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
IT and Technical Support	• Desarrollar y apoyar con la infraestructura IT que implica implementar y desmantelar el hardware, software y los sistemas operativos para el ejercicio practico • 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 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
- Linea 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. Un resumen ejecutivo sera entregado a ITU-IMPACT para futuros reportes.
