Concurso CAPTURE THE FLAG - EPN

3a Edición

1. Indicaciones Generales

- Cada equipo estará conformado por dos integrantes, mismos que necesariamente deben ser estudiantes universitarios de pregrado.

2. Primera Fase

Se dispondrá de una cantidad de retos a ser resueltas por los equipos participantes, los retos abordarán áreas relacionadas a seguridad en aplicaciones web, criptografía, esteganografía, codificación, malware, informática forense, entre otras.

Al resolver cada reto correctamente se otorgará a cada equipo participante de una bandera para registrarla en la plataforma provista e ir acumulando puntos.

MECÁNICA DE LA FASE:

- La plataforma presentará los retos a resolverse.
- Al ser validada correctamente la bandera por los organizadores, se adjudicará una cantidad de puntos a la cuenta del equipo.
- Se dispondrá de un tablero de puntos para que los equipos puedan observar sus puntos adjudicados en tiempo real.
- Los equipos dispodrán de 30 minutos para la resolución de los retos, al finalizar ese lapso la plataforma se cerrará y se asignarán los puntajes respectivos.

3. Segunda Fase

- Los organizadores del concurso entregarán a cada equipo un servidor virtualizado en VMWare Workstation 11.1.0 para que sea blindado, mismo que tendrá preinstalado los servicios FTP, WEB, VNC, SSH, y una base de datos Mysql.
- Cada equipo debe traer sus propias computadoras (laptops).

- Dos por equipo, una para atacar y otra para instalar el servidor virtualizado a ser defendido (debe tener instalado VMWare Workstation 11.1.0 o versiones superiores).

- Cada equipo es encargado de proteger su servidor y atacar a los sistemas de sus contrincantes.
  - Son libres de emplear las herramientas de ataque que cada equipo considere necesarias (traer previamente instaladas).
  - Cada equipo contará con acceso a Internet para descargar las herramientas de defensa y/o ataque.
- Todas las acciones de ataque y defensa referentes al concurso se realizarán dentro de la red que será entregada por los organizadores. Dicha red será controlada y separada de la infraestructura de la EPN.

MECÁNICA DE LA FASE:

- Fase de aseguramiento:
  - Inicialmente, cada equipo contará con un tiempo máximo de 45 minutos para asegurar al servidor virtualizado. Durante el tiempo establecido, cada equipo conectará su servidor a la red de la Escuela Politécnica Nacional para acceder a Internet y asegurar su sistema.
  - Por ningún motivo se permite cambiar los puertos de los servicios instalados en el servidor virtualizado.
  - Una vez transcurrida la fase de aseguramiento, cada equipo debe conectar su servidor a la red suministrada para que sea visible por los demás equipos atacantes.
- Fase de ataque:
  - Únicamente el equipo que tenga conectado su servidor virtualizado para ser atacado tendrá derecho a realizar ataques sobre otro equipo.
  - El ataque por denegación de servicio no es permitido en esta fase del concurso.
  - El tiempo máximo de ataque será de 90 minutos.
- Fase de resultados:
  - El ganador es aquel equipo cuyo servidor permanezca operativo. (La página web debe ser accesible y se debe poder realizar consultas a la base de datos).
  - Para declarar al ganador en caso de que más de un servidor permanezca operativo, los organizadores evaluarán las vulnerabilidades descubiertas y explotadas para cada equipo.

4. Lugar:

Facultad de Ingeniería Eléctrica y Electrónica (6 Piso), Laboratorio de informática de la FIEE.

5. Fecha y hora:

Jueves 20 de Julio de 2017

Hora de Registro: 8:20 – 8:50.

Hora de concurso: 09h00 12:00.

6. Inscripciones:

Las inscripciones se recibirán hasta el domingo 16 de Julio de 2017 a través del siguiente enlace: https://goo.gl/s1FXY6

Reglas para el día del concurso:

- Cada miembro del equipo deberá portar un documento de identificación que contenga su fotografía y un documento que certifique ser estudiante universitario de pregrado.
- Se puede usar recursos impresos como libros, manuales, apuntes e Internet.
- Para que un equipo entre a concursar deben estar los dos miembros del equipo presentes.
- Durante el concurso no pueden recibir ayuda de un tercero.
- No se permiten actos deshonestos, o no éticos.
- Bajo ninguna circunstancia los equipos deberán atacar al servidor en donde se aloja la plataforma de retos.
    - Cualquier consideración extra será evaluada por la organización y dada a conocer a todos los equipos.
    - El no cumplimiento de las reglas se traducirá en la expulsión del equipo participante.

7. Ayuda para la preparación:

Se recomienda practicar con el sistema vulnerable Metasploitable 2, disponible en Internet.

8. Costos:

La actividad es completamente gratuita.

9. Premios:

El primer y segundo lugar serán premiados y a todos los participantes se les hará la entrega de diplomas de participación.

10. Contacto:

En caso de requerir mayor información, puede dirigir sus inquietudes a:
concursodetri@epn.edu.ec