CRONOGRAMA DE CONFERENCIAS

www.openhacking.org

Hora	Tema	Conferencista	País
07.30am	**Registro en mesa técnica de asistentes al evento**		
07.50am	**Palabras de inauguración de Open Hacking Guatemala**		
08am a 09am	Trape: the phishing evolution	Jose Pino	Colombia
09am a 10am	El Robo de dinero a través de un Malware bancario	Jaime Restrepo DRAGONJAR	Colombia
10am a 11am	Robo de códigos de segunda autenticación (2FA) en aplicaciones bancarias a través de aplicaciones maliciosas en dispositivos móviles	Omar Jacobo Muñoz	Guatemala
11am a 12pm	Memorias de un perito informático forense vol. $((iv + i))	Lorenzo Martínez Rodríguez (Webinar)	España
12pm a 01pm	**ALMUERZO**		
01pm a 02pm	Magia, Innovación y Pensamiento Hacker Versión 2.0	Juan Pablo Quiñe Paz	Perú
02pm a 03pm	Los nuevos retos y desafíos de la ciberseguridad en el sector Bancario	Rafael Bucio Velázquez	México
03pm a 04pm	Mitigación de ataques en infraestructuras críticas	Estefani Olvera	México
04pm a 05pm	Análisis Forense a Malware de Criptominería	Alvaro Andrade Sejas	Panamá
05pm a 06pm	Anatomía forense de un ataque remoto a cajeros automáticos - pruebas de campo y reinicio de los cajeros	Kenneth López Orozco	Guatemala
06.10pm	Clausura del Evento		

TENDREMOS UN TALLER en paralelo al evento principal que inicia de 02pm a 06pm (solo 30 cupos)

Taller de Capacitación Hands On para el Manejo de Incidentes de Seguridad Informática: Gestión de un Ataque Pishing

Coordinado por : Ing. José Luis Chávez Cortéz (Guatemala)
Incluirá los siguientes temas:

1. Manejo de Incidentes de Seguridad Informática.
2. Manejo de información sensible / Gestión de la información.
3. Caso de estudio para el manejo adecuado de la información sensible.
4. Comprender/Entender los conceptos de: Confidencialidad, Integridad y Autenticidad.
5. Entender/Comprender lo que significa un ataque informático y en particular los del tipo Pishing.
6. Manejo de Roles y estándares en equipos especializados que administran incidentes de seguridad informática.
7. Uso de herramientas informáticas definidas en el taller bajo un ambiente de red creado para el evento.
8. Es un taller del tipo vivencial (hands on) que permitirá desdibujar lo que significa en la realidad la vida de los distintos

Contáctanos en el (502) 58666403 / 59360666 o escríbenos a capacitaciones@infogtm.com

CRONOGRAMA DE CONFERENCIAS

www.openhacking.org

profesionales en informática y como administrar la visión del técnico bajo ataque.

9. Temas implicados: creación de informes, análisis de vulnerabilidad, pruebas de penetración, manejos de incidentes, trabajo en equipo, conocimiento técnico, administrativo y gerencial.

El taller tiene como motivación el poder identificar en dónde está el hacker y poder armar un relato completo del tipo forense que denote lo que realmente sucedió.

PARTICIPANTES

Podrán ingresar su laptop para poder acceder al ambiente operativo creado para el taller.

METODOLOGÍA DEL TALLER

Los participantes se dividirán en 5 grupos compuestos por 6 personas, cumpliendo cada uno de ellos el rol de un centro de respuesta a incidentes de seguridad informática (esto permite que todos los participantes tengan actividades que realizar).

El instructor guiará a los participantes y cumplirá con los roles externos a los centros de respuesta involucrados en el incidente, proveyendo a cada grupo la información necesaria para avanzar en la resolución del caso.

Cada centro de respuesta deberá analizar la información entregada por el instructor y en función de ella, redactar las comunicaciones, tanto sean requerimientos de información, notificaciones o recomendaciones que fueran necesarias y dirigirlas a los otros centros de respuesta o a las distintas entidades externas que se encuentren involucradas.

El ejercicio planteará, en forma paralela, dos variantes de ataque de phishing similares. Luego, los cuatro equipos deberán interactuar entre sí motivados por la ocurrencia en sus territorios de distintos eventos vinculados con el ataque.

Los mismos equipos de trabajo, analizarán el caso de estudio presentado para el manejo de información sensible y harán presentación de lo que ellos consideran que debió de cumplirse. Para finalizar se presentarán las conclusiones respectivas y directivas necesarias para el cumplimiento satisfactorio de la actividad vivencial.

¿A QUIEN ESTÁ DIRIGIDO?

Participantes que tengan un conocimiento/experiencia en los siguientes temas:

Auditores/Técnicos en Seguridad Informática.

Administradores de Red y de Sistemas.

A quienes deseen orientar su carrera profesional hacia el campo de la seguridad informática de los distintos sistemas de información.

DURACIÓN

El Taller tendrá una duración de 03 horas y media.