



] SECTF [

] Normativa [



] NORMATIVA [

Antes de registrarte, es necesario que leas atentamente la normativa. Cualquier incumplimiento de la misma supondrá la inmediata descalificación.

La norma más importante de esta competición es la de mostrar total respeto hacia todas las partes implicadas.

Por tanto, es imprescindible que demostréis el máximo respeto hacia la empresa objetivo y sus trabajadores, no utilizando métodos intimidatorios ni denigrantes.

Las habilidades de ingeniería social se pueden demostrar sin necesidad de utilizar técnicas poco éticas.

Os recordamos que nuestro objetivo es generar concienciación sobre las técnicas de ingeniería social.

Si incumples cualquiera de las normas especificadas en esta lista, recibirás una amonestación o incluso podrías ser expulsado de la competición.

Cuestiones a considerar :\>

- Para poder registrarte en la competición, deberás ser mayor de edad.
- A cada participante le será enviado por email un dossier con el nombre y la URL de la empresa que le ha sido asignada, así como una lista con las flag y su correspondiente puntuación.
- El participante se compromete a no revelar el nombre de la empresa que le ha sido asignada.
- Antes del congreso, los participantes deberán conseguir tanta información sobre la empresa como les sea posible de fuentes públicas de información u OSINT (Open-source intelligence), como Google, LinkedIn, la web de la empresa, Facebook, Twitter, etc.



- Los participantes tienen prohibido comunicarse con la empresa, con la intención de obtener información, antes del evento.
- Está permitido llamar a los teléfonos que obtengas durante la fase de OSINT única y exclusivamente para garantizar que estén operativos el día de las llamadas.
- No está permitida la intrusión física, ni técnica (Red, servidores, etc.) en las empresas.
- Cada participante deberá redactar un informe con aspecto profesional con la información obtenida durante la fase de OSINT. Se enviará un informe de ejemplo a los participantes, que podrán usar como orientación para desarrollar el suyo. Gran parte de la puntuación dependerá de la calidad de este informe.
- Esperamos que hagáis un informe suficientemente trabajado, que incluya las conclusiones obtenidas tras analizar toda la información obtenida.
- El contenido del informe será puesto a disposición de la empresa correspondiente en caso de que así lo solicite.
- Cada flag que obtengas y que documentos debidamente en el informe durante la fase de OSINT, tendrá la mitad de su valor. Durante la fase de llamadas, tendrás la posibilidad de volver a obtener las flag, esta vez por su valor total.
- Los participantes dispondrán de tres semanas para completar la fase de OSINT y redactar el informe.
- Los participantes deberán enviar el informe antes de la finalización del día indicado en el dossier que les será entregado al inicio de la primera fase. La entrega injustificada en fecha posterior a la indicada supondrá la descalificación directa.
- No olvides venir a la fase de llamadas con tus pretextos bien preparados. Te recomendamos que los empieces a trabajar a lo largo de la primera fase, y los perfecciones desde la entrega del informe hasta el momento de tus llamadas durante el congreso.



- Durante el espacio de tiempo asignado al participante en el congreso, dispondrá de 20 minutos para realizar las llamadas, en una sala con un aforo aproximado de 30 personas. Durante las llamadas, deberá conseguir tantas flag como le sea posible. Las flag obtenidas durante esta fase tendrán valor total.
- El participante podrá tener disponible la personalización del identificador de llamada, si así lo solicita. El participante debe indicar claramente en una tabla incluida en el informe, el número al que quiere llamar y el identificador de llamada que quiere utilizar.
- Todos los números de teléfono facilitados deberán pertenecer al Plan Nacional de Numeración Telefónica, y no podrán ser números especiales o "inteligentes", ni números cortos.
- La puntuación final dependerá de los puntos obtenidos durante ambas fases, además de la puntuación subjetiva de los jueces respecto a la calidad del informe y los posibles vectores de ataque que haya propuesto el participante en su informe.
- El informe final realizado por la organización, no incluirá ninguna información que permita identificar a las empresas que han participado en la iniciativa, ni a los participantes.
- Deberás estar en la ceremonia de entrega de premios el último día del congreso. Si no, no podremos celebrar contigo la victoria :)

Está explícitamente prohibido :\>

- Intentar obtener información confidencial o personal (DNI, números de tarjetas de crédito, contraseñas, etc.)
- Utilizar técnicas que hagan pensar a las personas con las que se contacte que están en riesgo de algún tipo.
- Hacerse pasar por miembros de instituciones gubernamentales o fuerzas de seguridad.



- Llamar a personas que no sean empleados de la empresa objetivo.
- Utilizar "amistades" internas en la empresa objetivo para obtener información privilegiada.
- Llamar a los empleados a sus casas o números móviles personales.
- El uso de lenguaje grosero o amenazador, o cualquier técnica de ingeniería social agresiva.
- Hacerse pasar por personas que existen en el mundo real.
- Utilizar pretextos basados en el ofrecimiento de regalos o recompensas.

Usa el sentido común. Si te parece que algo puede ser poco ético, no lo hagas, y si tienes dudas pregunta a los jueces

La participación en este reto, supone la aceptación de la normativa por parte del participante y exime a la Asociación de Seguridad Informática EuskalHack de toda responsabilidad en caso de su incumplimiento.

Para cualquier duda o aclaración: <sectf@euskalhack.org>