

Tesi Camp
2022

Tesichallenge
2022



INSTRUCCIONES



Bienvenidos a esta nueva versión del TESICAMP, el mejor evento para demostrar tus habilidades dentro del área de computación. En este año, te presentamos la modalidad de Ciberseguridad, que se enfocará mas hacia el área Forense, en donde tendrás 3 retos distintos para poder resolver y demostrar tus habilidades para resolver casos, el Tesi Challenge esta dividido en **tres** etapas donde se tienen que presentar las respuestas a cada caso, además, el jurado evaluará la resolución en cada una de sus respuestas presentadas, por lo tanto, para conseguir la mejor puntuación, debes presentar primero las respuestas, además de la justificación de las mismas.

Van a existir horarios para poder presentar cada una de las respuestas y también los horarios en los cuales serán presentados los nuevos retos para resolver, de modo que, el ganador del reto será el que obtenga la mayor puntuación.

Liberación de retos:

Reto 1: Después de la conferencia “Aplicación de la computación cuántica en la industria 4.0”. 11:30 Aprox.

Reto 2: Después de la conferencia “La inteligencia artificial y el aprendizaje profundo: actualidad y futuro”. 17:30 Aprox.

Reto 3: Después de la conferencia “How to become a Cyber Security Professional?”. 23 Hrs. Aprox.

Entrega de soluciones: La entrega será vía correo electrónico: retos.tesicamp@gmail.com

Reto 1: 24 Noviembre a las 18:00 hrs. (Limite para la entrega)

Reto 2: 24 de noviembre a las 23:59 hrs. (Límite para la entrega)

Reto 3: 25 de noviembre a las 6:00 hrs. (Limite para la entrega)

25 noviembre a las 8:00 hrs, se harán una serie de preguntas referentes a los 3 retos. (Se compartirá el link de acceso)

Los puntajes máximos de cada reto sera de 100 puntos, por lo tanto, un récord perfecto seria alcanzar los 300 puntos, pero no te confíes, no será tan sencillo el poder llegar al final de los retos.

Recuerda que no estas solo, hay mas Tesi Hermanos tratando de ser los mejores, así que, sin mas preámbulo te dejamos el primer caso.

RETO 1.

- Como todo en este mundo de la informática forense inicia con una problemática, vamos a probar que tan involucrados están en esta área de especialización. Iniciaremos con algo sencillo, hemos detectado que se han utilizado de manera ilegal algunos scripts dentro de la empresa Orient Star y esto ha ocasionado que los servidores tengan un tráfico de datos que se considera inusual por parte de los administradores de red, se sabe que los involucrados trabajan bajo codificaciones en base 64, pero se detectó que se comunican a través de mensajes de spam codificados que no hemos podido descifrar, en el último análisis e incautación que realizamos, solo nos pudimos dar cuenta que el equipo que se utiliza genera volúmenes de datos muy grandes y el personal de TI de la empresa logró captar unos mensajes de spam dentro de la bandeja de reciclaje que se presenta a continuación.
- **Tu primera misión asignada es, decodificar el mensaje, analizar los scripts, entregar reporte de análisis , el tipo de lenguaje en que están codificado y determinar el por qué se generan los grandes volúmenes de datos.**
- **Se anexa el mensaje de txt en la siguiente URL.**
https://www.mediafire.com/file/wy2ke5r6204puh9/mensaje_spam.txt/file