TESI

Tesi Camp 2022

Reto 3

Tesichallenge 2022

Muy buen trabajo, parece ser que tienen un buen adiestramiento en la parte forense, vamos con la siguiente misión.

Necesitamos detectar cual es el servidor final del correo abuse@netmyne.com, las direcciones IP por las cuales pasa la trama de datos y la geolocalización del servidor, además de los 2 países anteriores por los cuales pasa el paquete de datos antes de llegar al destino final, lo único que tienes como evidencia es la cabecera que hemos detectado como sospechosa en algunas investigaciones realizadas previamente por un equipo de forenses y que se te adjunta para realizar la investigación correspondiente.

Misión 3 Analizar el header sospechoso y resolver las preguntas que se te cuestionan, puedes usar la herramienta de eMailTrackerPro para apoyarte con tus investigaciones, documentar tus respuestas.

Entrega de soluciones: La entrega será vía correo electrónico: retos.tesicamp@gmail.com
Reto 3: 25 de noviembre a las 6:00 hrs. (Limite para la entrega)

- **Header Capturado.**

Return-Path: <martinsmith61725@gmail.com>

Received: from WINO47CO6C2WXY ([202.75.54.101]) by mx.google.com with ESMTPS

id ml4sm80554665pbc.0.2011.09.26.21.42.30 (version=TLSv1/SSLv3 cipher=OTHER);

Mon, 26 Sep 2011 21:42:31 -0700 (PDT)

Message-ID: <4e815437.64d1440a.6fe9.4fad@mx.google.com>

Date: Mon, 26 Sep 2011 21:42:31 -0700 (PDT)

From: Microsoft Outlook <martinsmith61725@gmail.com>

To: =?utf-8?B?bWFydGluc21pdGg=?= <martinsmith61725@gmail.com>

Subject: =?utf-8?B?TWljcm9zb2Z0IE91dGxvb2sgVGVzdCBNZXNzYWdl?=

MIME-Version: 1.0

Content-Type: text/html; charset="utf-8"

Content-Transfer-Encoding: 8bit