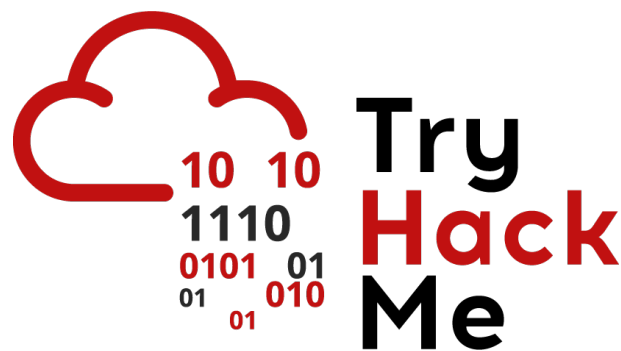


Writeup: Sala *Phishing Analysis Fundamentals*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 – Introducción	2
2.2. Tarea 2 - La dirección de correo electrónico	2
2.3. Tarea 3 - Entrega de correo electrónico	3
2.4. Tarea 4 - Encabezados de correo electrónico	3
2.5. Tarea 5 - Cuerpo de un correo electrónico	5
2.6. Tarea 6 - Tipos de Phishing	7
2.7. Tarea 7 - Conclusion	12
3. Conclusión sobre la Sala	12

1. Introducción

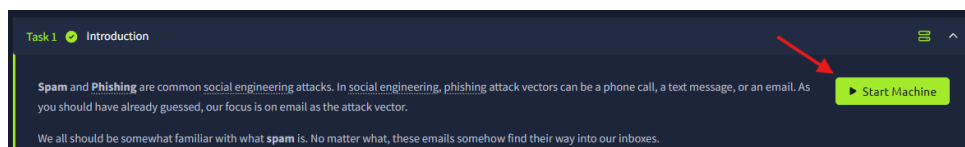
En esta sala aprenderemos a identificar elementos clave de un correo electrónico, como las direcciones, encabezados, cuerpos y archivos adjuntos, con el objetivo de detectar posibles amenazas. Además, conoceremos los diferentes tipos de phishing, sus características y cómo distinguirlos.

2. Sala

2.1. Tarea 1 – Introducción

En esta primera tarea aprenderemos que el phishing es como una técnica de ingeniería social fundada mayormente en correos electrónicos. Resalta que, a pesar de tener defensas robustas, un usuario inexperto que haga clic en un enlace o ejecute un adjunto malicioso puede permitir que un atacante ingrese en la red corporativa.

Antes de continuar con las siguientes tareas, se debe desplegar la máquina virtual proporcionada por TryHackMe para resolver las preguntas de tareas posteriores. Para el despliegue de la máquina, haremos clic en **Start Machine** en el lado superior de la tarea.



Pregunta: Read the above and launch the attached VM.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - La dirección de correo electrónico

Aprenderemos sobre la anatomía de una dirección de correo como

- El nombre del buzón (usuario)
- El símbolo @
- Dominio (por ejemplo, usuario@dominio.com)

También, conoceremos brevemente los orígenes en ARPANET durante la década de 1970.

Después de comprender la dirección de correo electrónico, pasamos a responder las siguientes preguntas.

Pregunta: Email dates back to what time frame?

Respuesta: 1970s

2.3. Tarea 3 - Entrega de correo electrónico

Conoceremos sobre los tres protocolos clave del correo electrónico:

- **SMTP (Simple Mail Transfer Protocol)**
- **POP3 (Post Office Protocol)**
- **IMAP (Internet Message Access Protocol)**

Además, vamos a aprender sobre el viaje de un correo desde que se envía hasta que llega al cliente, mencionando puertos seguros (SMTP-465, IMAP-993 y POP3-995)

Una vez entendido la entrega de un correo electrónico, pasamos a responder las siguientes preguntas.

Pregunta: What port is classified as Secure Transport (STARTTLS) for SMTP?

Respuesta: 587

Pregunta: What port is classified as Secure Transport for IMAP?

Respuesta: 993

Pregunta: What port is classified as Secure Transport for POP3?

Respuesta: 995

2.4. Tarea 4 - Encabezados de correo electrónico

En esta tarea, vamos a enfocarnos en los encabezados visibles como:

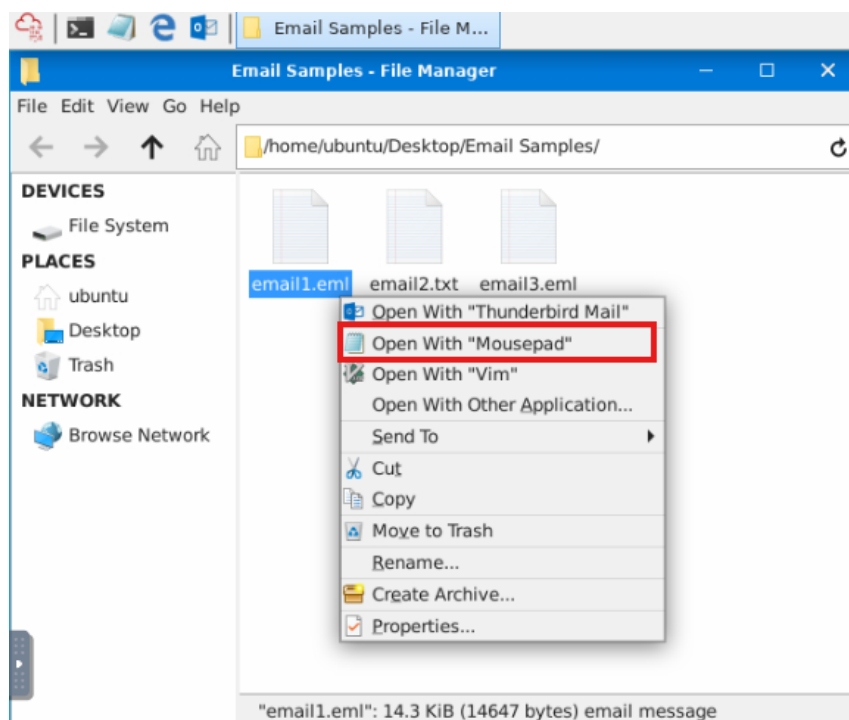
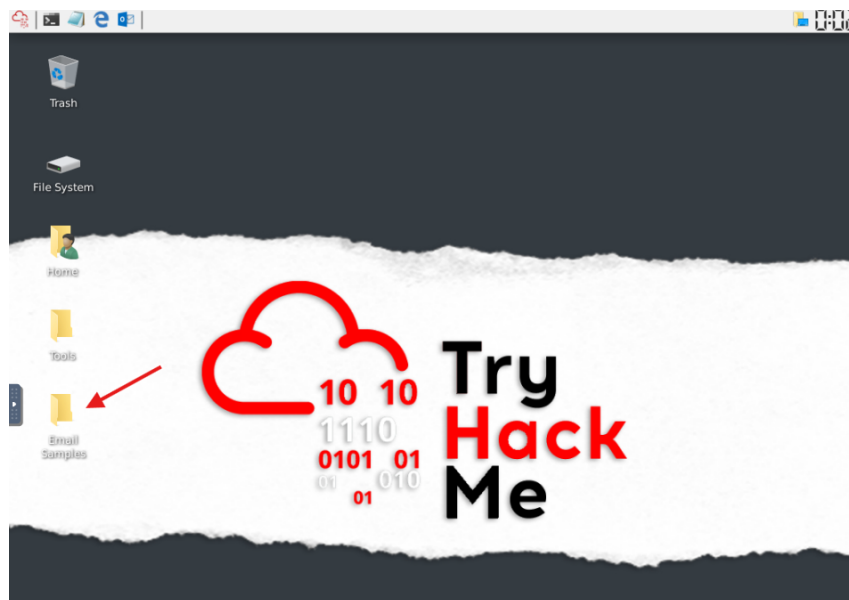
- **From**
- **To**
- **Subject**
- **Date**

Posterior a eso, aprenderemos sobre X-Originating-IP (IP origen), Reply-To/Return-Path (para respuestas), y campos de autenticación relacionados con el dominio. Por último, cómo usar ARIN para investigar una IP.

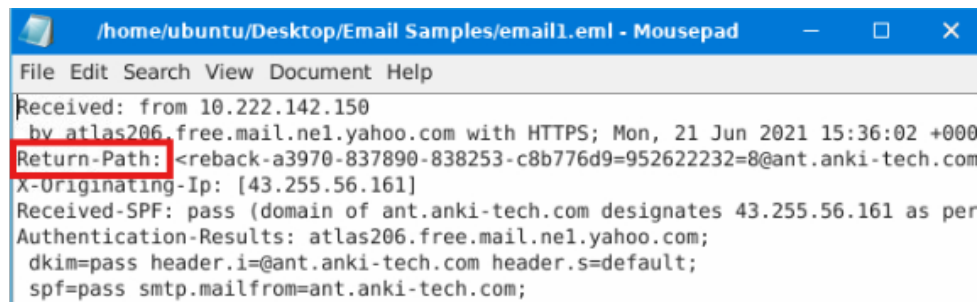
Una vez que comprendemos los encabezados de un correo electrónico, pasamos a responder las siguientes preguntas.

Pregunta: What email header is the same as Reply-to?

Para encontrar la respuesta, iremos a nuestra máquina virtual levantada previamente (En tarea 1) y abriremos la carpeta **Email Samples**, luego, abriremos con la opción de Mousepad el archivo **Email1.eml**.



Analizando bien el archivo, podremos encontrar que el encabezado de respuesta es **Return-Path**



```
/home/ubuntu/Desktop/Email Samples/email1.eml - Mousepad
File Edit Search View Document Help
Received: from 10.222.142.150
  by atlas206.free.mail.ne1.yahoo.com with HTTPS; Mon, 21 Jun 2021 15:36:02 +000
Return-Path: <reback-a3970-837890-838253-c8b776d9=952622232=8@ant.anki-tech.com>
X-Originating-Ip: [43.255.56.161]
Received-SPF: pass (domain of ant.anki-tech.com designates 43.255.56.161 as per
Authentication-Results: atlas206.free.mail.ne1.yahoo.com;
dkim=pass header.i=@ant.anki-tech.com header.s=default;
spf=pass smtp.mailfrom=ant.anki-tech.com;
```

Respuesta: **Return-Path**

Pregunta: Once you find the email sender's IP address, where can you retrieve more information about the IP?

Respuesta: <http://www.arin.net>

2.5. Tarea 5 - Cuerpo de un correo electrónico

Aprenderemos cómo analizar el cuerpo en HTML de un correo, mostrando cómo ver imágenes, enlaces y adjuntos a través del código fuente. También, vamos a aprender los headers como Content-Type, Content-Disposition y Content-Transfer-Encoding (como base64) y cómo reconstruir un adjunto codificado (por ejemplo, un PDF benigno) para extraer su contenido.

Ahora que sabemos analizar un cuerpo de correo con HTML, procederemos a responder las siguientes preguntas.

Pregunta: In the above screenshots, what is the URI of the blocked image?

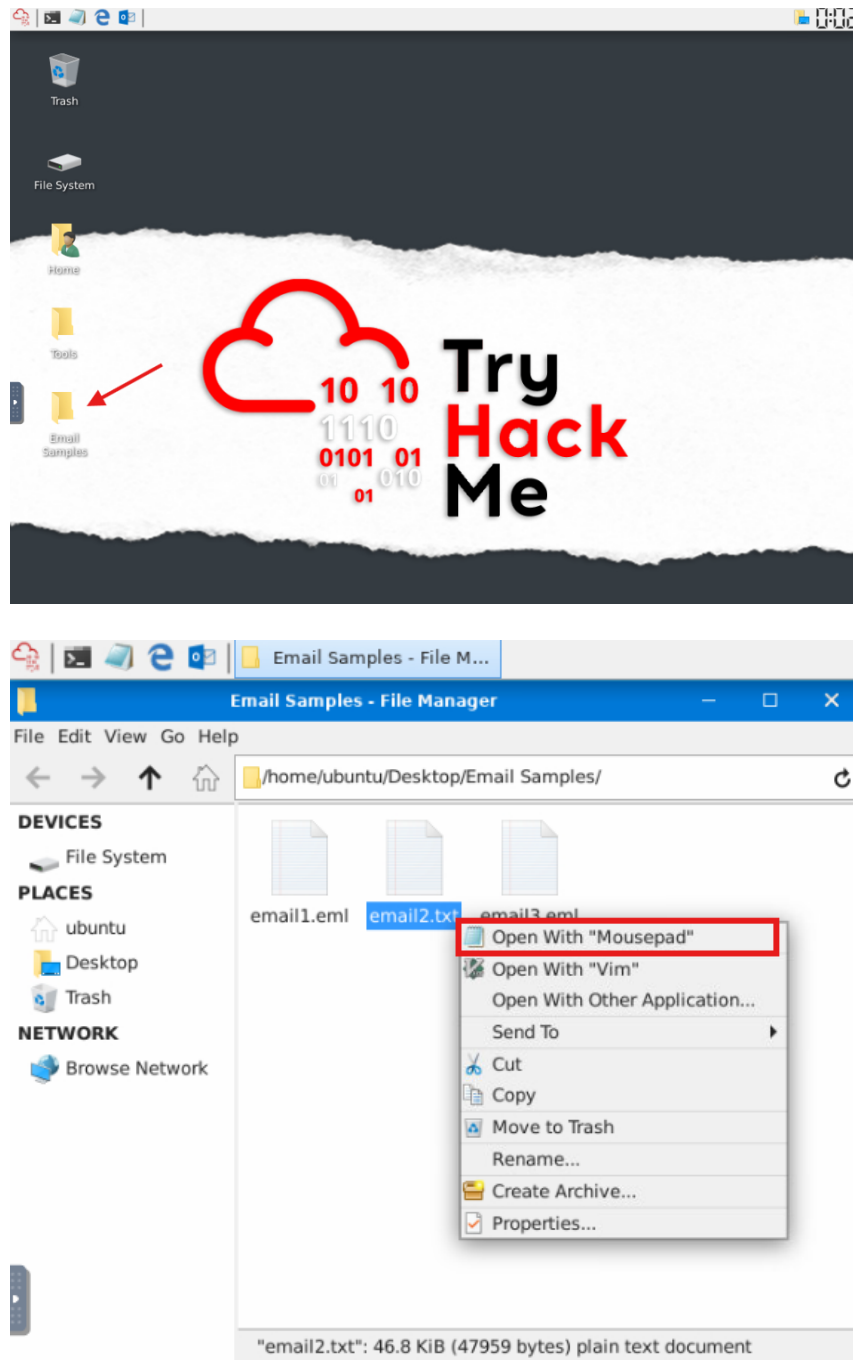
Respuesta: <https://i.imgur.com/LSWOtDI.png>

Pregunta: In the screenshots above, what is the name of the PDF attachment?

Respuesta: **Payment-updateid.pdf**

Pregunta: In the attached virtual machine, view the information in email2.txt and reconstruct the PDF using the base64 data. What is the text within the PDF?

Para encontrar el texto en el PDF, iremos a la carpeta **Emails Samples** en la máquina virtual y abriremos el archivo **Email2.txt** con la opción de Mousepad.



Una vez abierto el archivo, copiaremos toda la cadena de texto en base64 y buscaremos en un navegador web una herramienta para convertir [base64 a PDF](#).

[Comments: 132](#) | [Rating: 4.6/5](#)

- Name: Portable Document Format
- Developer: Adobe Inc.
- MIME types: application/pdf, application/x-pdf, application/x-bzpdf, application/x-gzpdf
- File Extensions: .pdf
- Uniform Type Identifier: com.adobe.pdf

Comments: 132 | Rating: 4.6/5

[illegible][illegible]

7

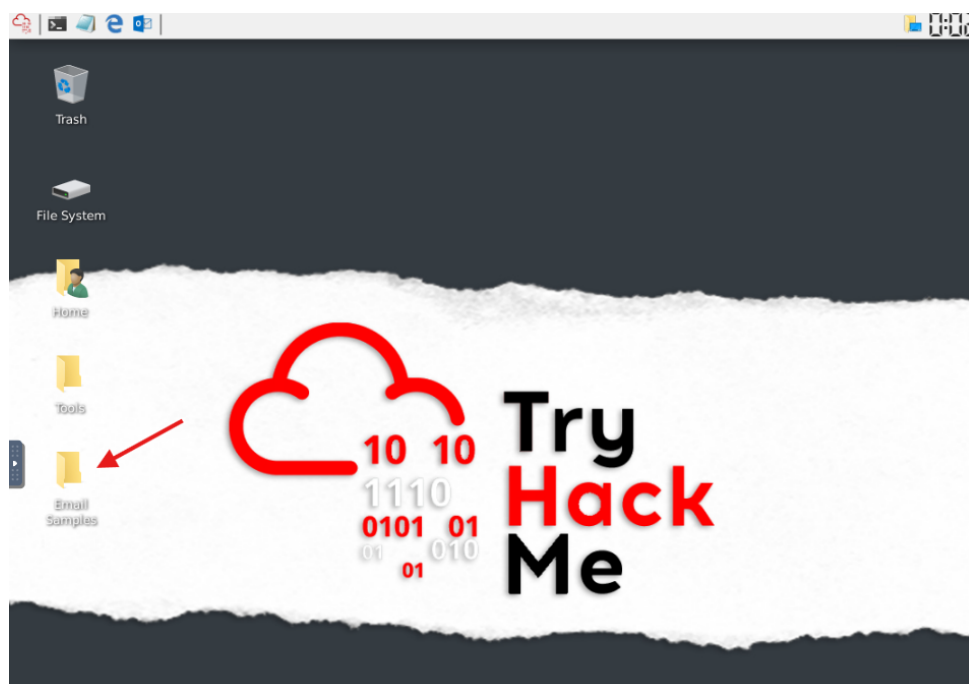
- Spam
- MalSpam
- Phishing
- Spear Phishing
- Whaling
- Smishing
- Vishing

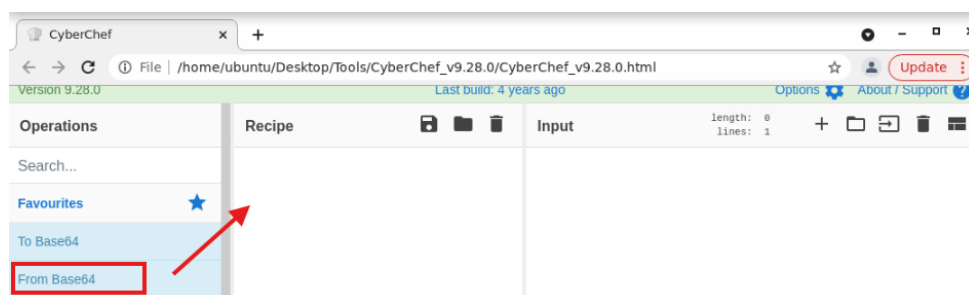
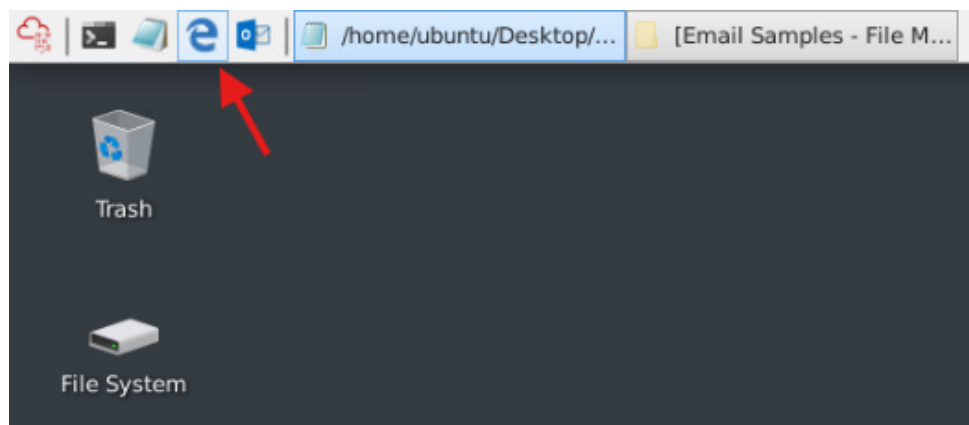
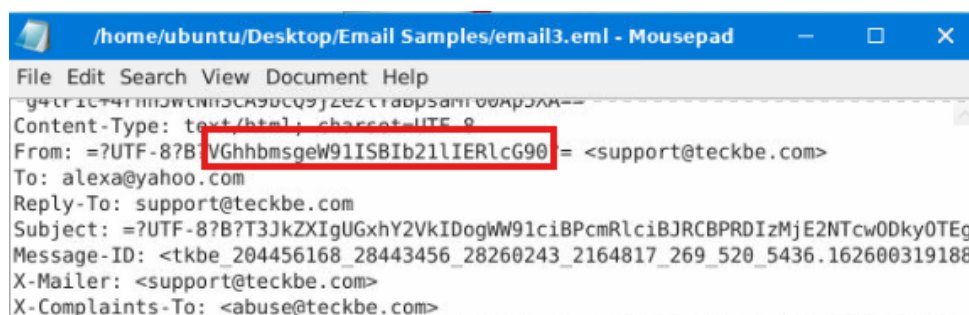
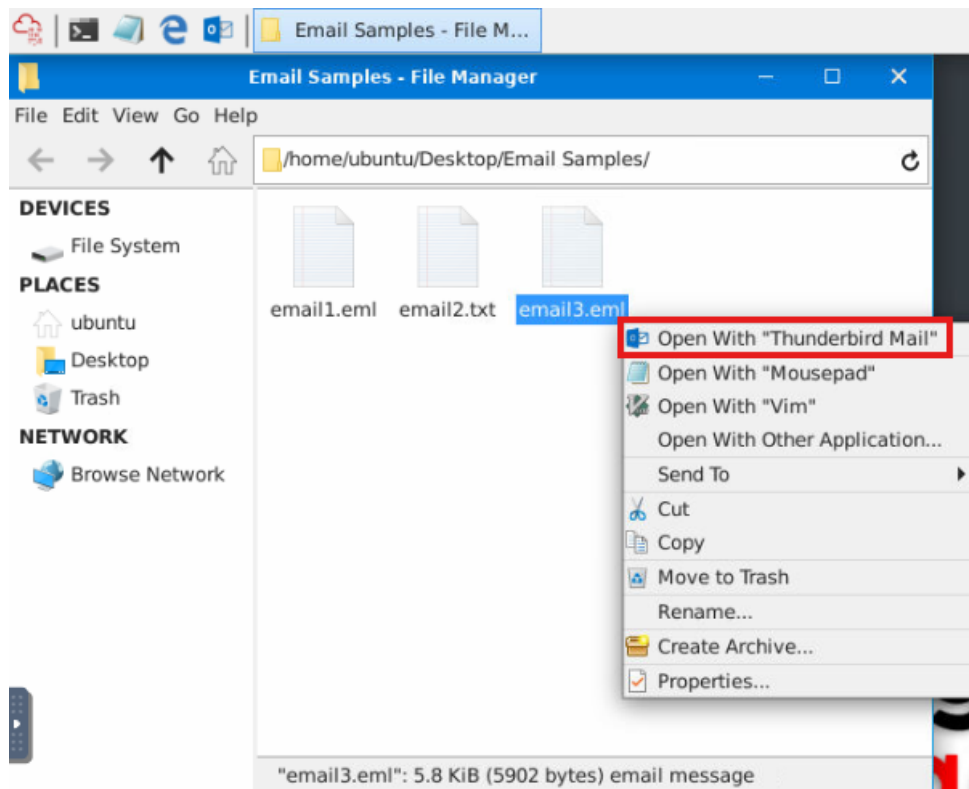
También aprenderemos las tácticas comunes como suplantación de remitente, lenguaje urgente, formatos engañosos, contenido genérico, URLs acortadas o maliciosas y adjuntos falsos. Por último, el proceso de **defanging** para neutralizar enlaces e IPs.

Una vez entendido los distintos tipos de Phishing, procederemos a responder las siguientes preguntas analizando el correo **emil3.eml** de la máquina virtual.

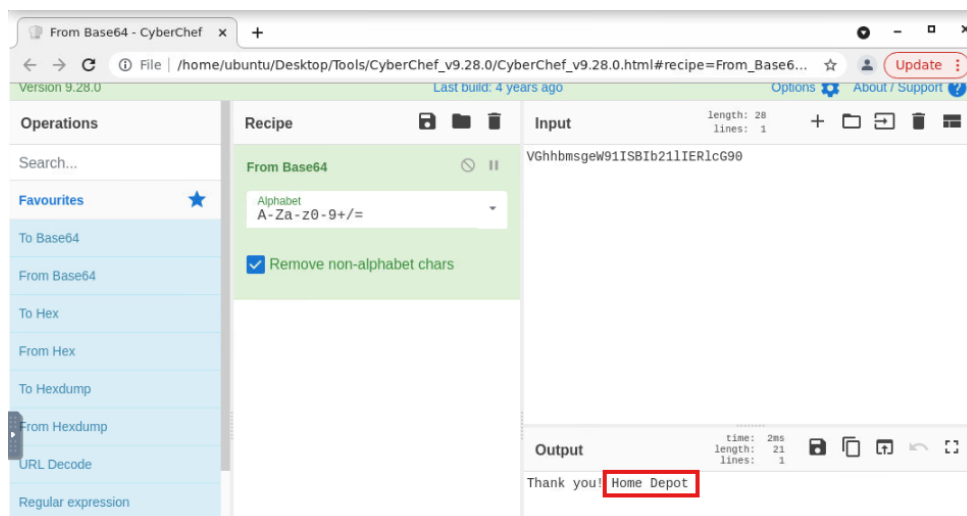
Pregunta: What trusted entity is this email masquerading as?

Para encontrar la respuesta, debemos ir a la carpeta **Email Samples** y abrir el archivo **Email3.eml** con la opción Mousepad. Una vez abierto vamos a leer y analizar a profundidad el archivo. Notaremos que en la sección **From** tendremos una cadena de texto base64 la cual copiaremos, posterior a eso, haremos uso de la herramienta **CyberChef** que para ingresar a ella haremos clic en el icono de **Internet Explorer**.





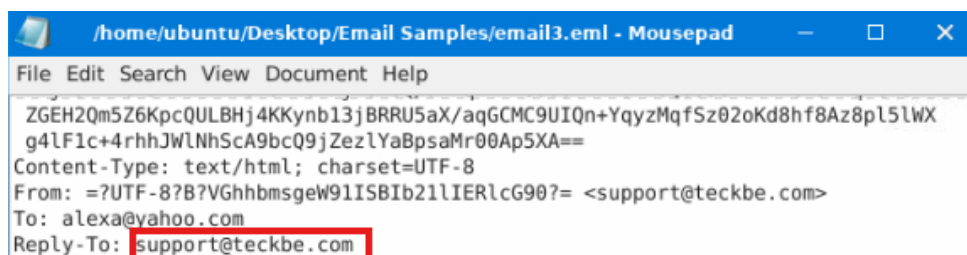
Una vez abierta la herramienta, arrastraremos la opción **From base64** en Recipe y pegaremos en Input la cadena en base64 para obtener la respuesta



Respuesta: Home Depot

Pregunta: What is the sender's email?

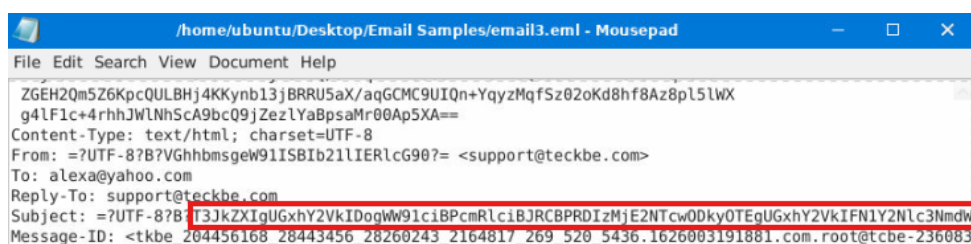
Encontraremos la respuesta analizando el archivo nuevamente y en la opción **Reply To** encontramos el correo.

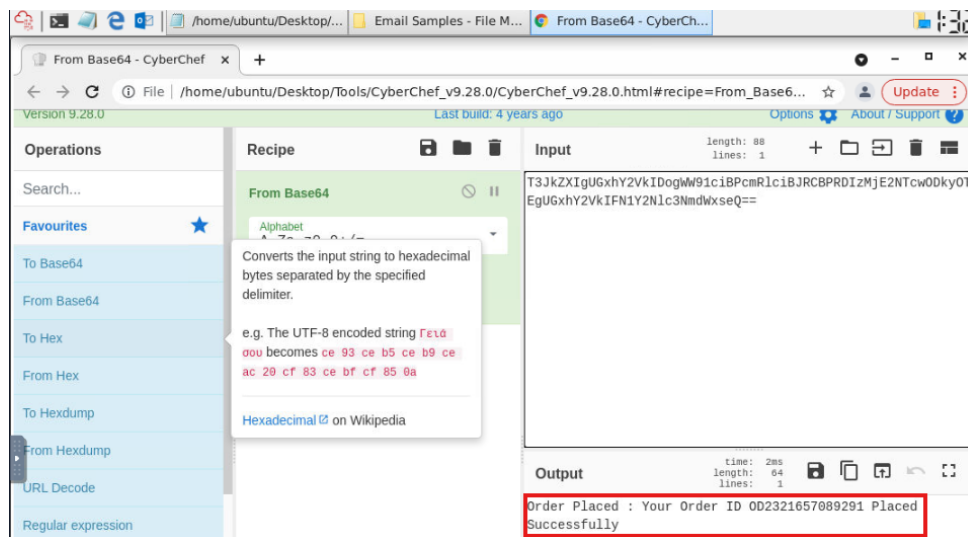


Respuesta: support@teckbe.com

Pregunta: What is the subject line?

Para saber que dice el Subject debemos ir al archivo y en la opción de **Subject** copiaremos la cadena de texto en base64 y la pegaremos en el Input del CyberChef para obtener la respuesta.

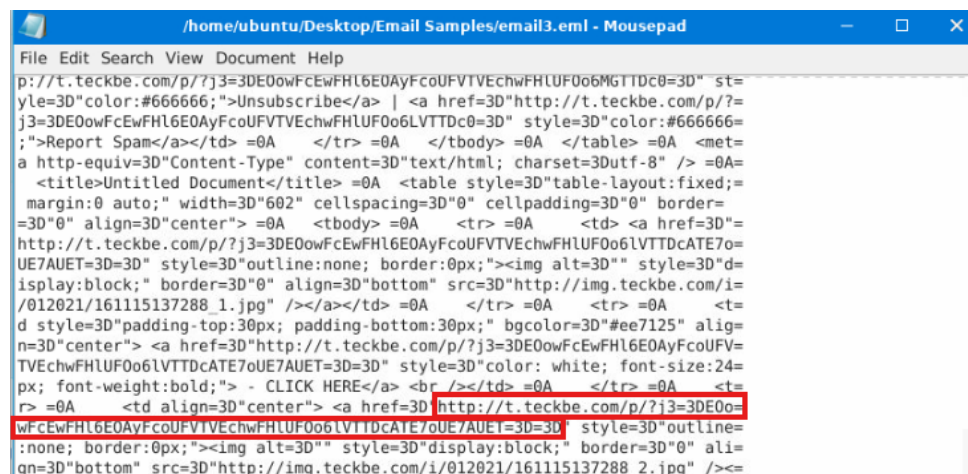


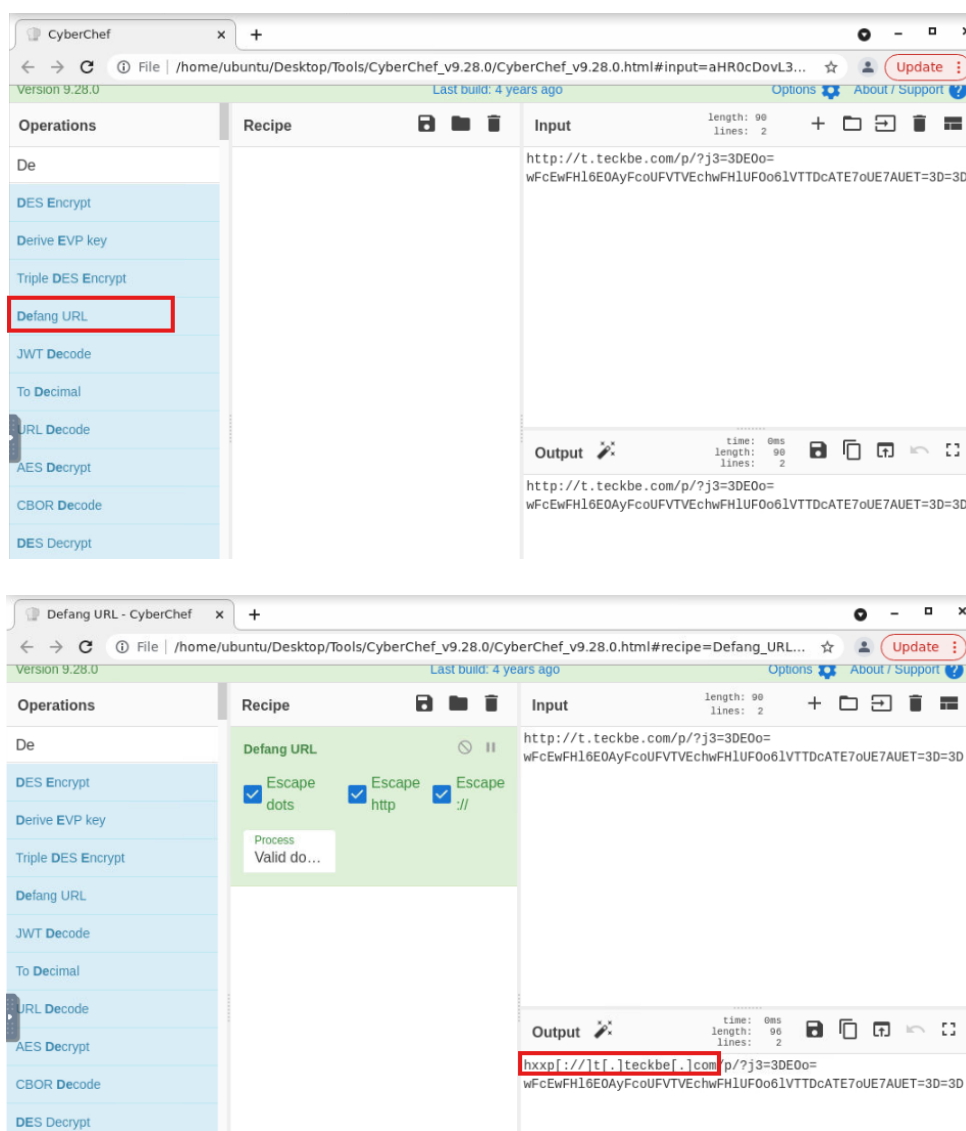


Respuesta: Order Placed : Your Order ID OD2321657089291 Placed Successfully

Pregunta: What is the website for the - CLICK HERE URL in a defanged format? (e.g. https://website.thm)

Para encontrar la respuesta debemos analizar el cuerpo HTML del archivo y encontrar la URL de CLICK HERE. Una vez encontramos la URL en el href procedemos a copiar la dirección e iremos al CyberChef y cambiaremos la opción a **Defang URL** y pegaremos la cadena de texto en Input para obtener la respuesta.





Respuesta: **hxxp[://][t[.]teckbe[.]com**

2.7. Tarea 7 - Conclusion

En esta última tarea aprenderemos el significado de **BEC (Business Email Compromise)** y cuando ocurre.

Pregunta: What is BEC?

Respuesta: **Business Email Compromise**

3. Conclusión sobre la Sala

Finalizamos la sala logrando obtener conocimientos fundamentales para analizar correos electrónicos sospechosos, reconociendo señales típicas de ataques de

phishing. También, aprendimos sobre los protocolos de envío y recepción, la interpretación de cabeceras, el análisis de cuerpos en HTML y la identificación de adjuntos maliciosos.