Fundamentos del análisis de phishing

Tarea 1: Introducción

El spam y el phishing son ataques comunes de ingeniería social . En ingeniería social , los vectores de ataque de phishing pueden ser una llamada telefónica, un mensaje de texto o un correo electrónico. Como ya habrás adivinado, nos centramos en el correo electrónico como vector de ataque.
Todos deberíamos estar familiarizados con lo que es **el spam** . Sea como sea, estos correos electrónicos llegan a nuestras bandejas de entrada de alguna manera.
El primer correo electrónico clasificado como spam data de 1978 y sigue vigente hoy en día.
El phishing es un vector de ataque serio contra el cual usted, como defensor, tendrá que defenderse.
Una organización puede seguir todas las pautas recomendadas para desarrollar una estrategia de defensa por capas. Sin embargo, basta con que un usuario inexperto e incauto dentro de su entorno corporativo haga clic en un enlace o descargue y ejecute un archivo adjunto malicioso que podría proporcionar a un atacante una vía de acceso a la red.
Muchos productos ayudan a combatir el spam y el phishing , pero siendo realistas, estos correos electrónicos aún pueden filtrarse. Cuando esto sucede, como analista de seguridad, necesitas saber cómo analizarlos para determinar si son maliciosos o inofensivos.
Además, necesitará recopilar información sobre el correo electrónico para actualizar sus productos de seguridad y evitar que correos electrónicos maliciosos regresen a la bandeja de entrada de un usuario.
En esta sala, veremos todos los componentes involucrados en el envío de correos electrónicos a través de Internet y cómo analizar los encabezados de correo electrónico.

P: Lea lo anterior e inicie la máquina virtual adjunta.
R: No se necesita respuesta

Tarea 2: La dirección de correo electrónico
P: ¿A qué período de tiempo se remonta el correo electrónico?
R: 1970s

Tarea 3: Entrega de correo electrónico
P1: ¿Qué puerto está clasificado como Transporte Seguro (STARTTLS) para SMTP?
R1: 587

P2: ¿Qué puerto está clasificado como Transporte Seguro para IMAP?
R2: 993

P3: ¿Qué puerto está clasificado como Transporte Seguro para POP3?
R3: 995

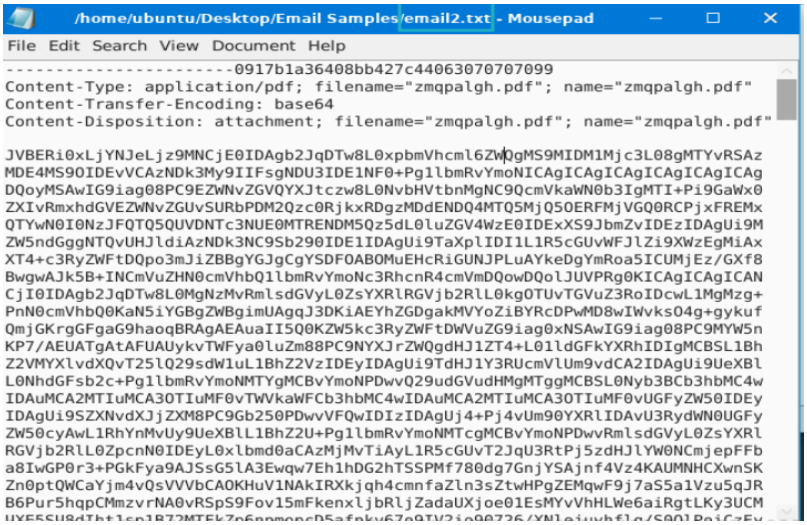
Tarea 4: Encabezados de correo electrónico
P1: ¿Qué encabezado de correo electrónico es igual a "Responder a"?
R1: Return-Path / Ruta de retorno

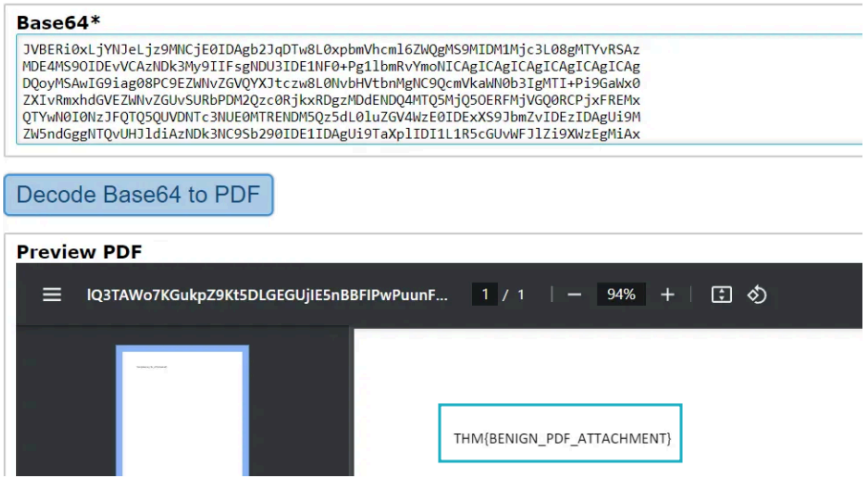
P2: Una vez que encuentre la dirección IP del remitente del correo electrónico, ¿dónde puede obtener más información sobre la IP?
R2: http://www.arin.net

Tarea 5: Cuerpo del correo electrónico
P1: En las capturas de pantalla anteriores, ¿cuál es la URI de la imagen bloqueada?
R1: https://i.imgur.com/LSWOtDI.png

P2: En las capturas de pantalla anteriores, ¿cuál es el nombre del archivo PDF adjunto?
R2: Payment-updateid.pdf

P3: En la máquina virtual adjunta, visualice la información en email2.txt y reconstruya el PDF con los datos base64. ¿Qué texto contiene el PDF?





R3: THM{BENIGN_PDF_ATTACHMENT}

Tarea 6: Tipos de phishing
P1: ¿En qué entidad confiable se hace pasar este correo electrónico?
R1: Home Depot

P2: ¿Cuál es el correo electrónico del remitente?
R2: support@teckbe.com

P3: ¿Cuál es el asunto?
R3: Order Placed : Your Order ID OD2321657089291 Placed Successfully

P4: ¿Cuál es el sitio web para la URL - HAGA CLIC AQUÍ en un formato desvanecido? (por ejemplo, https://website.thm)
R4: hxxp[://]t[.]teckbe[.]com

Tarea 7: Conclusion
P: ¿Qué es BEC?
R: Business Email Compromise

💼**LinkedIn:**https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/
💻 **GitHub:** https://github.com/MaateoSuar