Common Attacks

Tarea 1: Introducción
P: ¡Comencemos!
R: No se necesita respuesta

Tarea 2: Ingeniería social
P1: Lea la información de la tarea y mire los videos adjuntos.
R1: No se necesita respuesta

P2: ¿Cuál era el objetivo original de Stuxnet?
R2: The Iran Nuclear Programme / El Programa Nuclear Iraní

Tarea 3: Ingeniería social: phishing
P1: Haga clic en el botón verde "Ver sitio" en la parte superior de esta tarea si aún no lo ha hecho.
R1: No se necesita respuesta

P2: El sitio estático mostrará una serie de correos electrónicos y mensajes de texto. Se le pedirá que identifique cuáles son genuinos y cuáles son intentos de phishing. Una vez que haya identificado todos los mensajes, se le mostrará una bandera para ingresar. ¡Buena suerte! . ¿Qué es la bandera?

Phishing Test 1:

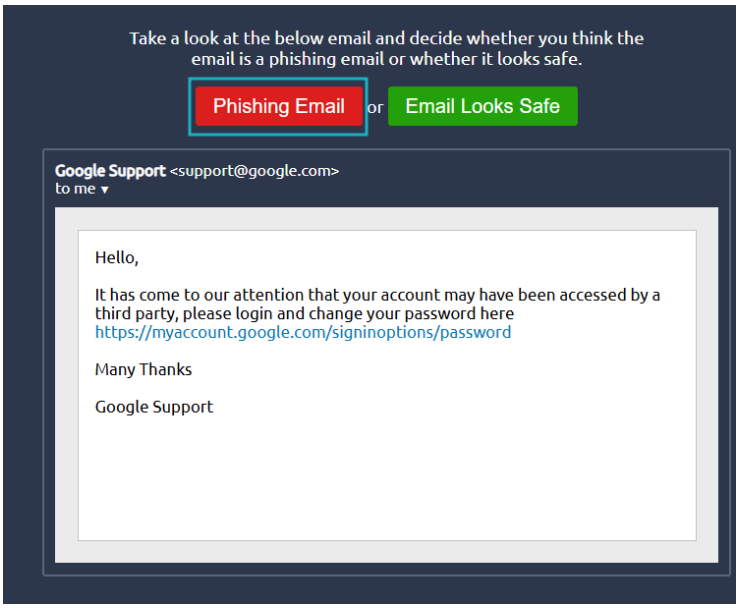

Figura 1 (Test 1)

Phishing Test 2:

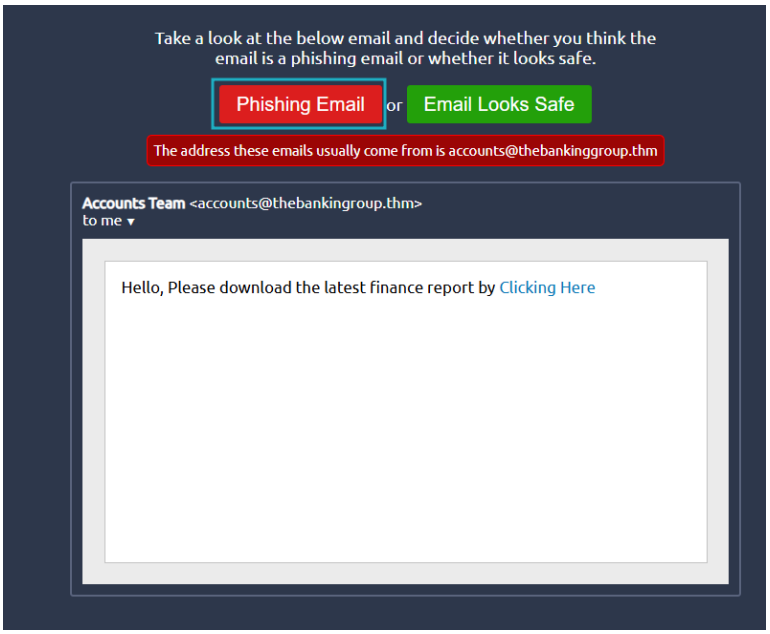

Figura 2 (Test 2)

Phishing Test 3:

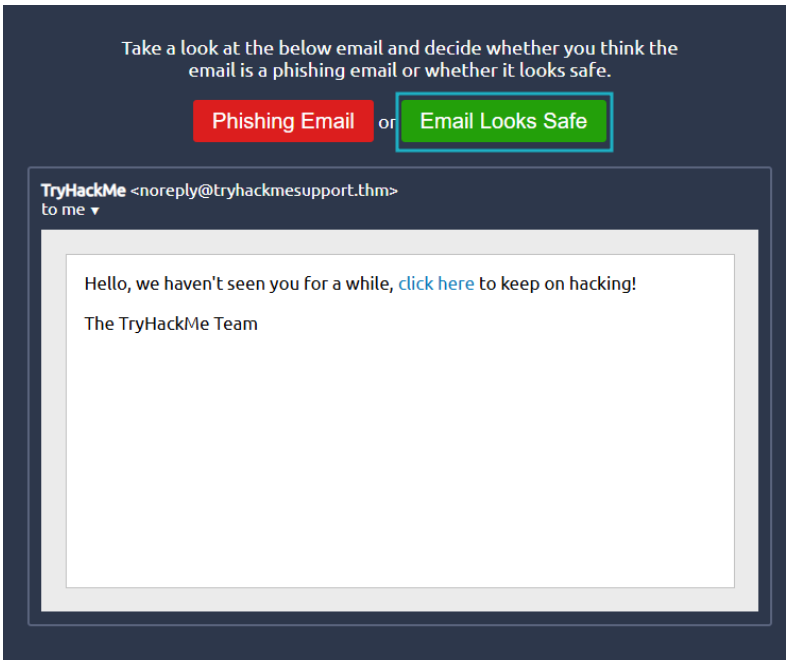

Figura 3 (Test 3)

Phishing Test 4:

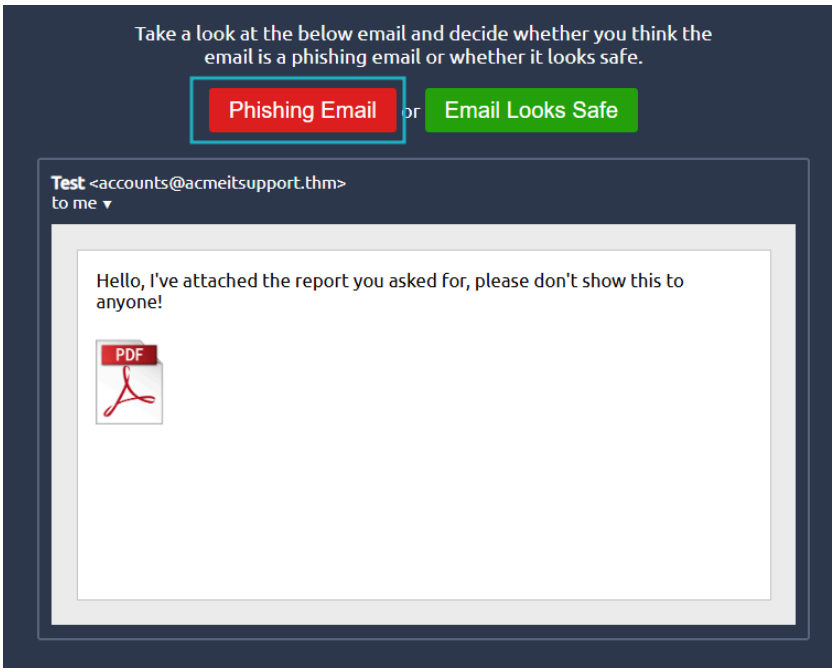

Figura 4 (Test 4)

Flag conseguida:

Figura 5 (Flag)

Tarea 4: Malware y ransomware
P: ¿En qué moneda solicitaron el pago los atacantes de Wannacry?
R: Bitcoin

Tarea 5: Contraseñas y autenticación
P1: Ponte en la piel de un hacker malicioso. Has conseguido acceder a la base de datos de contraseñas de un servicio en línea, ¡pero aún tienes que descifrar esos hashes!
¡Haga clic en el botón verde al comienzo de la tarea para implementar el forzador de hash interactivo!
R1: No se necesita respuesta

P2: Basándose en el contenido del sitio web, ha generado una lista de posibles contraseñas, que es la siguiente:
TryH@ckMe
TryHackMe123
THM123456
qwertyuiop123
TryHackMe2021
TryHackMe123!
TryHackMe345
TryHackM3!
Copie la lista de contraseñas en el campo "Lista de contraseñas" del descifrador de hash y luego haga clic en "Ir".
R2: No se necesita respuesta

P3: Mire la sección "Palabra actual / Hash" del descifrador de hash.
Tenga en cuenta que, para cada palabra de la lista ingresada, el descifrador crea un hash MD5 y lo compara con el hash objetivo. Si ambos hashes coinciden, ¡se ha encontrado la contraseña!. El descifrador de hash debería encontrar la contraseña que coincida con el hash objetivo muy rápidamente.¿Cual es la contraseña?

Ingresamos las posibles contraseñas:

Figura 1 (Lab)

Contraseña encontrada:

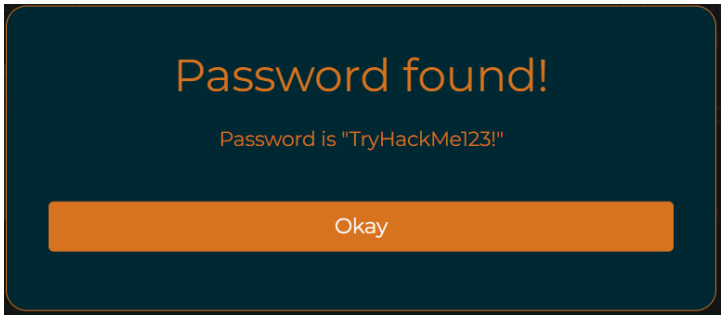

Figura 2 (Contraseña)

R3: TryHackMe123!

P4: Este es un ejemplo muy simple basado en navegador; sin embargo, en realidad, descifrar un hash local con una lista de palabras no es más complejo desde una perspectiva de alto nivel: es la misma técnica, pero con muchas más contraseñas potenciales.
Esperemos que este ejemplo ilustre por qué es tan importante elegir una contraseña segura, incluso si las contraseñas están codificadas correctamente.
En la siguiente tarea, veremos algunas de las medidas de protección de cuentas más comunes, así como también cómo generar contraseñas seguras.

R4: No se necesita respuesta

Tarea 6: Autenticación multifactor y administradores de contraseñas
P1: Cuando tenga la opción, ¿cuál debería utilizar como segundo factor de autenticación entre TOTP basados en SMS o TOTP basados en aplicaciones de autenticación (SMS o aplicación)?

R1: App

Tarea 7: Seguridad de la red pública
P1: Implemente el contenido interactivo haciendo clic en el botón verde en la parte superior de la tarea.
R1: No se necesita respuesta

P2: El contenido interactivo de esta tarea demuestra lo que puede ocurrir si se envía información a través de una red potencialmente insegura con varios tipos de cifrado (o sin ellos). No hay indicadores para esta tarea, pero se recomienda probar cada uno de los diferentes escenarios, combinando las opciones disponibles en el cuadro de control en la esquina inferior derecha de la pantalla.

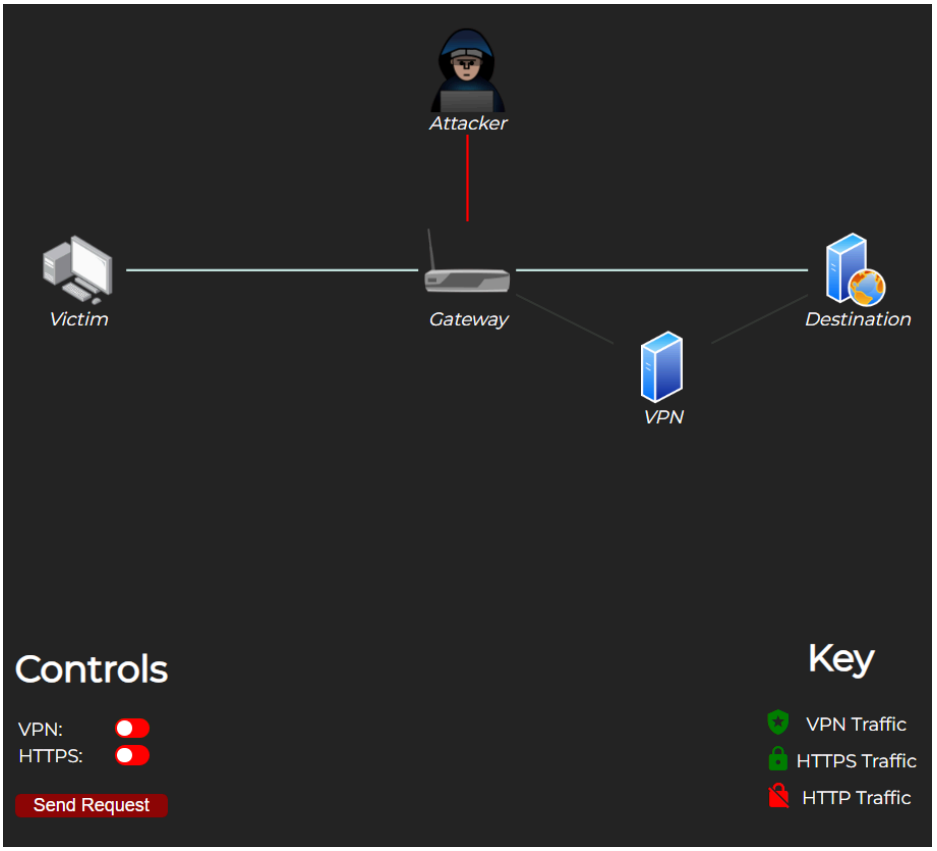

Figura 3 (Contenido Interactivo)

R2: No se necesita respuesta

Tarea 8: Copias de seguridad
P1:¿Cuál es el número mínimo de copias de seguridad actualizadas que debes realizar?
R1: 3

P2: De estos, ¿cuántos (como mínimo) deberían almacenarse en otra ubicación?
R2: 1

Tarea 9: Actualizaciones y parches
P:(Opcional) ¡Completa la sala azul en TryHackMe para ver tú mismo los efectos brutales del exploit Eternal Blue en acción contra una máquina sin parchear!

R: No se necesita respuesta

Tarea 10: Conclusión
P: ¡He completado la sala de Ataques Comunes!
R: No se necesita respuesta

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