Documentación Sala Common Attacks (Ataques Comunes)

Tarea 1: Introducción

Solo debemos presionar Complete.

Tarea 2: Social Engineering(Ingeniería Social)

Aca veremos lo que es la ingeniería social, las distintas formas de ingeniería social que existen y cómo protegerse de los ataques de ingeniería social. En la primera pregunta solo debemos presionar Complete.

Pregunta

What was the original target of Stuxnet?

Respuesta

The Iran Nuclear Programme

Tarea 3: Social Engineering: Phishing (Ingeniería Social: Phishing)

En este caso veremos la rama de la ingeniería social llamada phishing que sería más específicamente el envío de correo electrónico falso con el fin de robar credenciales.

1) Pregunta

   Hello,

   It has come to our attention that your account may have been accessed by a third party, please login and change your password here https://myaccount.google.com/signinoptions/password
   Many Thanks
   Google Support

   Respuesta

   Phishing mail

2) Pregunta

   Hello, Please download the latest finance report by Clicking Here

   Respuesta

   Phishing mail

3) Pregunta

   Hello, we haven't seen you for a while, click here to keep on hacking!
   The TryHackMe Team

   Respuesta

   Email Looks Safe

4) Pregunta

   Hello, I've attached the report you asked for, please don't show this to anyone!

   Respuesta

   Phishing mail

Esto nos dará la FLAG para responder la siguiente pregunta.

Pregunta

The static site will display a series of emails and text messages. You will be asked to identify which of these messages are genuine and which are phishing attempts.
Once you have successfully identified all of the messages you will be presented with a flag to enter, here.
Good luck!
What is the flag?

Respuesta

THM{I_CAUGHT_ALL_THE_PHISH}

Tarea 4: Malware and Ransomware

Veremos lo que es un malware y un ransomware, que efectos tiene y para que se usan, así mismo vamos a aprender cómo defendernos de estos tipos de ataques.

Pregunta

Research] What currency did the Wannacry attackers request payment in?

Respuesta

Bitcoin

Tarea 5: Passwords and Authentication(Contraseñas y Autenticación)

Conoceremos cual es la forma más efectiva y segura de crear una contraseña y también cuáles no lo son. Así también vamos a conocer sobre otras formas de ayudar a la contraseña a ser más segura.

Pregunta

Look at the "Current Word / Hash" section of the hash cracker.
Notice that for each word in the list you entered, the cracker is creating an MD5 hash of the word then comparing it to the Target Hash. If the two hashes match then the password has been found!
The hash cracker should find the password that matches the target hash very quickly.
What is the password?

Respuesta

TryHackMe123!

Tarea 6: Multi-Factor Authentication and Password Managers(Autenticación Multi-Factor y Administradores de Contraseñas)

Acá veremos que es un autenticador y cuáles son los más seguros que existen en el mercado.

Pregunta

Where you have the option, which should you use as a second authentication factor between SMS based TOTPs or Authenticator App based TOTPs (SMS or App)?

Respuesta

App

Tarea 7: Public Network Safety(Seguridad de Redes Públicas)

Acá vamos a conocer lo importante del uso de seguridad en las redes públicas, como el uso de VPN para no permitir que un atacante nos intervenga.

Solo debemos presionar Complete.

Tarea 8: Backups (Copias de Seguridad)

conoceremos cuantas copias de seguridad debemos tener usando la regla 3,2,1, la importancia de esto y donde almacenar las copias.

Pregunta

What is the minimum number of up-to-date backups you should make?

Respuesta

3

Pregunta

Of these, how many (at minimum) should be stored in another location?

respuesta

1

Tarea 9: Updates and Patches (Actualizaciones y Parches)

Veremos la importancia de tener actualizado tanto los sistemas como las aplicaciones, también sobre la actualización de antivirus y el caso Eternal Blue.

Solo debemos presionar Complete.

Tarea 10: Conclusión

Para concluir: hay muchas opciones diferentes para que un atacante malicioso apunte tanto a individuos como a grupos radicales; sin embargo, hay remediaciones para cada ataque. Solo debemos presionar Complete.