1. La verdad detrás de los *Hackers*

2. Datos personales

Autor: Martín Amorín

Centro educativo: SEK – Atlántico (Poio)

3. Resumen del proyecto

Mi proyecto consistió en crear una serie de videos que recogiesen los aspectos más importantes del trabajo de un hacker, ejemplificando situaciones reales.

Desde un principio no sabía muy bien que formato darles y dónde publicarlos, pero después de mucho reflexionar e inspirarme de otros creadores de contenido, me decidí por YouTube.

Ya tenía mucha información al respecto, pero lo más difícil no fue obtener la información, sino ser capaz de sintetizarla, y difundirla de forma que la gente que no conociese tanto el tema fuese capaz de entenderlo, ya que la ciberseguridad es un tema un poco complejo.

Además de todo esto, tuve la suerte de contar con la colaboración de un forense informático que trabaja para la policía, y entrevistarlo para apoyar mi proyecto.

4. Introducción

Hace un tiempo a un amigo le vulneraron el acceso a su cuenta de Instagram, a mí me mató la curiosidad de ver como alguien fue capaz de burlar la seguridad de una de las redes más famosas del mundo.
Después de eso sentí el deber de difundir esa información para evitar que a más gente le pase esto.

5. Propósito del trabajo

Desde el principio yo sabía que quería hacer un video, porque considero que son la forma de difusión más completa y comprensible. Luego de elaborar los videos, quería subirlos a YouTube, para que así pudiese llegar a todo el mundo. Pero antes de todo eso, tenía que reunir toda la información que quería incluir, pese a que yo ya tenía unas nociones básicas de ciberseguridad, tenía que aprender algunas cosas más, para poder hacer un producto lo más

completo posible. Los videos tenían que incluir ejemplos de vulneración real, para que así la gente se diese cuenta de cómo actúa un cibercriminal, y lo fácil que es que te vulneren tu dispositivo móvil.

Además, tuve la suerte de contar con la ayuda de Santi Rey, un forense informático que, desde su experiencia, nos contaba casos reales sobre los hackers.

6. Estudio del estado del arte

Para inspirarme utilicé canales como el de s4vitar qué es un divulgador de este tipo de conocimiento, me fije en el formato de sus videos y como explicaba, pero yo no quería que mis videos fuesen tan técnicos, así que también me inspire de canales de entretenimiento general como pueden ser Nil OGT o Ibai.

Para el entorno de SO decidí usar Parrot ya que es un sistema hecho totalmente para ciberseguridad y es muy cómodo. Las herramientas que usé fueron HiddenEye para hacer phishing, ya que es una herramienta básica pero con mucho potencial y además es muy cómoda de usar.

El proceso para vulnerar el server lo saque de aquí, y todas las herramientas se ven durante el proceso.

7. Hipótesis

Si consigo llevar a cabo pequeños vídeos divulgativos sobre los peligros asociados a Internet y la forma de actuación del hackers que sean lo suficientemente técnicos pero accesibles y comprensibles para cualquiera, seré capaz de concienciar a la población sobre este tema y conseguiré que los espectadores estén más concienciados de los peligros de internet.

8. Material y métodos

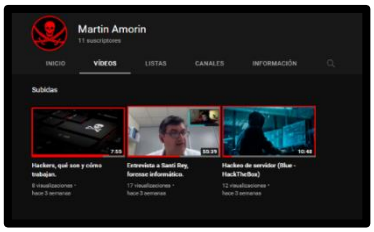
En cuanto a materiales se refiere, mi proyecto utiliza mucho las herramientas de Software como pueden ser:

- OBS Studio: para la grabación y edición de videos.
- Adobe Premiere Pro: para la edición de video.
- Un ordenador.
- Un micrófono

- Distribución de Linux Parrot OS.

Y en cuanto a la metodología, para producir los videos me basaba en tres fases:

a. Recopilación de información.
b. Guionización de los videos.
c. Grabación y edición



9. Resultados

Al final creo que logré alcanzar a hacer unos videos de calidad, y que sobre todo cumplen con mi objetivo de difundir la información con facilidad, ya que las críticas fueron muy positivas, y todo el mundo que los alcanzó a ver fue capaz de entenderlos. Además, al haber dos videos, uno más complejo y otro más genérico, el usuario se adapta a su propio nivel de dificultad.

Link canal: https://www.youtube.com/@martinamorin203/

10. Conclusiones.

En conclusión, creo que he cumplido mi objetivo principal, sobre todo he aprendido mucho más sobre ciberseguridad, uso de herramientas propias de un Hacker como pueden ser HiddenEye, dnmasq o nmap. Además, he sido capaz de aprender a difundir conocimientos, porque pensaba que iba a ser mucho más fácil de lo que en realidad fue.

11. Bibliografía

Ch4p. (2017, 24 marzo). Blue - HackTheBox. HackTheBox. Recuperado 16 de febrero de 2022, de https://app.hackthebox.com/machines/Blue

M. (s. f.-a). GitHub - Morsmalleo/HiddenEye: Modern Phishing Tool With Advanced Functionality And Multiple Tunnelling Services [Android-Support-Available]. GitHub. Recuperado 27 de diciembre de 2021, de https://github.com/Morsmalleo/HiddenEye

W. (s. f.-b). GitHub - worawit/MS17-010: MS17-010. GitHub. Recuperado 16 de marzo de 2022, de https://github.com/worawit/MS17-010

Vázquez, M. (2020, 25 mayo). Introducción al Hacking ético. Mastermind. Recuperado 2 de enero de 2022, de https://www.mastermind.ac/courses/introduccion-al-hacking-etico