JuanpabloSalado

Nivel: 1
Tipo: individual
Modo: obligatorio
Dificultad: facil

Skootik Mobile Technologies

https://skootik.com
info@skootik.com

Tener un conocimiento genérico sobre cuales son las técnicas de ciberseguridad más usadas actualmente

Pentesting

¿Te has preguntado alguna vez quiénes son las personas que velan por la ciberseguridad de las empresas? Durante los últimos años el número de ciberataques ha aumentado significativamente debido a la proliferación de virus, malwares y técnicas cada vez más sofisticadas. El objetivo de estos ciberataques suele ser en muchas ocasiones la captación de información confidencial, tanto personal como corporativa. Toda empresa que tenga parte de su negocio digitalizado se enfrenta a riesgos que ponen en peligro sus intereses, y nadie está libre de estos peligros. Sin embargo, no todas las organizaciones son conscientes de los riesgos a los que se enfrentan y es por este motivo que las brechas de seguridad siguen creciendo.

Tener la capacitación de hacer frente a estas nuevas técnicas de ciberataque tan sofisticadas y en constante cambio son uno de los mayores retos de la ciberseguridad informática. Para proteger los sistemas digitales, es necesario que la ciberseguridad avance a la misma velocidad que lo hacen estas nuevas técnicas de ataque digital y es en este contexto donde surge el Pentesting.

Pentesting: Es una de las prácticas más novedosas en cuanto a ciberseguridad, que surge por los numerosos robos de información sufridos por numerosas empresas, alguna de ellas muy importante.

Un *pentest* o *test de penetración/intrusión*, es un método para poder evaluar los sistemas de información y la red digital de una organización simulando un ataque. Se refiere a un asalto lanzado desde la propia organización o proveedor para encontrar vulnerabilidades que permitan a potenciales atacantes robar información o afectar a sus activos (inyección SQL, malware, ataques DoS, etcétera). El propósito es analizar las medidas y controles de seguridad para detectar debilidades, fallos técnicos y vulnerabilidades.

Estas pruebas se realizan utilizando técnicas y herramientas similares o iguales a las que utilizan los atacantes, pero sin el ánimo de perjudicar a la organización. Los tests de intrusión realizados deben ir precedidas de un acuerdo firmado donde se defina el alcance del mismo, así como las restricciones y/o limitaciones de las pruebas. El *pentester* o *auditor de ciberseguridad* es una de las profesiones más demandadas dentro del mundo de la ciberseguridad.

¿Cómo se realiza una prueba de intrusión?

Se deben seguir unos pasos para garantizar un buen examen y para poder realizar todas las averiguaciones posibles sobre fallos o vulnerabilidades del sistema:

1.- Estas pruebas se deben realizar por personal especializado y debe ir cubierto por un acuerdo firmado donde se recoja el alcance y demás parámetros del test, así como acompañarlo con un acuerdo de confidencialidad (NDA). En esta fase el auditor debe evaluar con qué datos cuenta y qué tipo de prueba

va a realizar. Normalmente el cliente determina el tipo de información que puede ofrecer al analista y qué tipo de test quiere que se realice contra el sistema.
2.- Identificar y establecer los parámetros de la prueba: objetivos, limitaciones y justificación de los procedimientos y/o pruebas a realizar. El experto debe realizar varias pruebas para analizar las vulnerabilidades, fugas de información, etcétera. Utilizará varias herramientas y valorará aspectos clave para la selección de la estrategia más adecuada.
3.- Se seleccionarán las pruebas a realizar, se analizará de qué manera se va a actuar y directamente se organizan los ataques.
4.- Documentar los resultados de las pruebas detalladamente y hacer un informe para la audiencia a la que va dirigido. En el informe se deben recoger de una manera clara, concisa y exacta los hallazgos, el alcance e impacto de los fallos de seguridad atacados, así como las recomendaciones para poder minimizarlos o subsanarlos.

Tipos de pentesting

1.- Black Box: Los pentesters no disponen de conocimiento previo acerca de la infraestructura que va a ser probada. Es lo más parecido a un ataque real. Suele ser realizado por personal especializado externo a las organizaciones.
2.- Grey Box: Se parte con un conocimiento parcial previo de la infraestructura objetivo del test. Suele ser el tipo de pentest recomendado cuando se contrata a empresas especializadas.
3.- White Box: Test más completo ya que se parte de un conocimiento completo previo de la infraestructura. Normalmente lo realiza personal interno de las organizaciones o se contrata a alguien externo si la empresa no dispone de trabajadores especializados.

Se recomienda:
1.- Ver siguiente video: https://www.youtube.com/watch?v=roG3r5tNWOU. Es para haceros una idea, no os asustéis si no entendéis algunos conceptos y fragmentos de código. El objetivo de esta tarea es que tengáis una visión general. TheEgg no es una escuela de ciberseguridad.
2.- Mirar cual es tu ip pública. Para ello tienes un montón de webs que te dan esa información como por ejemplo: https://hidemy.name/es/what-is-my-ip/. Posteriormente ver qué puertos tienes abiertos por ejemplo aquí: https://hidemy.name/es/port-scanner/. Según este servicio que podemos encontrar en Internet, las normas de uso de su aplicación son las siguientes:

a. El escáner de puertos le permite encontrar PC-s y servidores en la red donde esté abierto el puerto. A menudo, los administradores verifican la disponibilidad de los puertos para encontrar debilidades en sus redes.
b. Un puerto abierto le permite conectarse al dispositivo desde Internet, si se está ejecutando un programa en este puerto que está listo para aceptar la conexión.
c. Nuestro escáner de puertos en línea se basa en la utilidad nmap más famosa, adaptada para la web.
d. Para verificar su computadora, haga clic en el botón "insertar mi dirección IP" al lado del formulario del escáner. No use el escáner para verificar servidores de terceros que no le pertenecen.

#HASHTAGS ***(etiquetas de ayuda para búsqueda de información relevante)***

#pentesting #pentester #pruebas-de-intrusión #ciberseguridad #DoS #Inyección-SQL #Phising #ransomware # spyware #troyano

LINKS DE INTERÉS

https://www.unir.net/ingenieria/revista/pentest/
https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting
https://www.youtube.com/watch?v=XZ9fy_4Eplw
https://www.youtube.com/watch?v=roG3r5tNWOU
https://hidemy.name/es/port-scanner/

DICCIONARIO

pentesting | ciberseguridad | ransomware | phising | spyware | troyano

PUNTUACIÓN

Programación: 1
Redes: 4
Seguridad: 8
Algoritmia: 2