**TAREA 40: DICCIONARIO**

* **PENTESTING:** Una prueba de penetración o pentest, es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. El proceso consiste en identificar el o los sistemas del objetivo. Las pruebas de penetración pueden hacerse sobre una “caja blanca” (donde se ofrece toda la información de fondo y de sistema) o caja negra (donde no se proporciona información, excepto el nombre de la empresa). Una prueba de penetración puede ayudar a determinar si un sistema es vulnerable a los ataques, si las defensas (si las hay) son suficientes y no fueron vencidas.

Los problemas de seguridad descubiertos a través de la prueba de penetración deben notificarse al propietario del sistema. Con los resultados de las pruebas de penetración podremos evaluar los impactos potenciales a la organización y sugerir medidas para reducir los riesgos.

Las pruebas de penetración son valiosas por varias razones:

* Determinar la posibilidad de éxito de un ataque
* Identificación de vulnerabilidades de alto riesgo que resultan de una combinación de vulnerabilidades de menor riesgo explotadas en una secuencia particular
* Identificación de vulnerabilidades que pueden ser difíciles o imposibles de detectar con red automatizada o un software de análisis de vulnerabilidades
* Comprobar la capacidad de los defensores de la red para detectar con éxito y responder a ataques.
* **XSS (Cross-site scripting):** Una secuencia de comandos en sitios cruzados es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en paginas web visitadas por el usuario código JavaScript o en otro lenguaje similar (VBScript). Se puede evitar usando medidas como CSP, política del mismo origen, etc;

Es posible encontrar una vulnerabilidad de XSS en aplicaciones que tengan entre sus funciones presentar la información en un navegador web u otro contenedor de paginas web. Sin embargo, no se limita a sitios web disponibles en Internet, ya que puede haber aplicaciones locales vulnerables a XSS, o incluso el navegador en sí.

XSS es un vector de ataque que puede ser utilizado para robar información delicada, secuestrar sesiones de usuario, y comprometer el navegador, subyugando la integridad del sistema. Las vulnerabilidades XSS has existido desde los primeros días de la Web.

Esta situación es habitualmente causada al no validar correctamente los datos de entrada que son usados en cierta aplicación, o no sanear la salida adecuadamente para su presentación como página web.

Esta vulnerabilidad puede estar presente de las siguientes formas:

* DIRECTA (también llamada Persistente): este tipo de XSS es comúnmente filtrado, y consiste en insertar código HTML peligroso en sitios que lo permitan; incluyendo etiquetas como <script> o <iframe>. Se utiliza para suplantación de identidad.
* INDIRECTA (también llamada Reflejada): este tipo de XSS consiste en modificar valores que la aplicación web utiliza para pasar variables entre dos páginas, sin usar sesiones y sucede cuando hay un mensaje o ruta en la URL del navegador, en una cookie, o cualquier otra cabecera HTTP (en algunos navegadores y aplicaciones web, esto podría extenderse al DOM del navegador). El PHISHING es un ejemplo de este tipo.
* **INYECCION SQL:** Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

El origen de la vulnerabilidad radica en la incorrecta comprobación o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase mas general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que este embebido dentro de otro.

Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

* **ATAQUE INFORMATICO:** También llamado Ciberataque, es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo. Un ataque informático, es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático. Utiliza códigos maliciosos, para corromper los códigos, datos privados o algoritmos, generando consecuencias que comprometen y vulneran la seguridad de los sistemas de información.
* **ATAQUE DDoS (Distributed Denia lof Service):** Ampliación del ataque DoS (Denial of Service) y es el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino. La forma más común de realizar un DDoS es a través de una red de bots, siendo esta técnica el ciberataque mas usual y eficaz por su sencillez tecnológica.

En ocasiones, esta herramienta ha sido utilizada como un buen método para comprobar la capacidad de trafico que un ordenador puede soportar sin volverse inestable y afectar los servicios que presta. Un administrados de redes puede así conocer la capacidad real de cada máquina.

Su método de ataque se basa en impedir el uso legitimo de los usuarios al usar un servicio de red. El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan la familia de protocolos TCP/IP para conseguir su propósito. Un ataque puede ser perpetrado de diferentes formas:

* Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
* Alteración de información de configuración, tales como información de rutas de encaminamiento.
* Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset)
* Interrupción de componentes físicos de red.
* Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.
* **INGENIERIA SOCIAL:** Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometidos. El principio que sustenta la ingeniería social es el de que, en cualquier sistema, los usuarios son el eslabón débil.

En la práctica, un ingeniero social usara comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a paginas web o correos electrónicos falsos que solicitan respuestas e incluso las famosas cadenas, llevando así a revelar sus credenciales de acceso o información sensible, confidencial o crítica.

Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

* **HACKER:** Todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo (según el diccionario de hackers). Comúnmente el termino es asociado a todo aquel experto de las tecnologías de comunicación e información que utiliza sus conocimientos técnicos en computación y programación para superar un problema, normalmente asociado a la seguridad. Habitualmente se les llama así a los técnicos e ingenieros informáticos con conocimientos en seguridad y con la capacidad de detectar errores o fallos en sistemas informáticos para luego informar los fallos a los desarrolladores del software encontrado vulnerable o a todo el público.
* **CRACKER:** Personas que rompen o vulneran algún sistema de seguridad de forma ilícita. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío. Mayormente, se entiende que los crackers se dedican a la edición desautorizada de software propietario. Sin embargo, debe entenderse que, si bien los ejecutables binarios son uno de los principales objetivos de estas personas, una aplicación web o cualquier otro sistema informático representan otros tipos de ataques que de igual forma pueden ser considerados actos de cracking.
* **MAN IN THE MIDDLE (Ataque de intermediario):** En criptografía, es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos victimas y procurar que ninguna de las victimas conozca que el enlace entre ellos ha sido violado. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando este se emplea sin autenticación. Hay ciertas situaciones donde es bastante simple, por ejemplo, un atacante dentro del alcance de un punto de acceso wifi sin cifrar, donde este se puede insertar como intermediario.

Existen varios tipos de defensa contra estos ataques MitM que emplean técnicas de autenticación:

* Claves públicas
* Autenticación mutua fuerte
* Claves secretas (secretos con alta entropía)
* Contraseñas (secretos con baja entropía)
* Otros criterios, como el reconocimiento de voz u otras características biométricas.
* **PHISHING:** El termino phishing es utilizado para referirse a uno de los métodos mas utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

El phisher se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.