Instituto Politécnico Nacional

Centro de Estudios Científicos y Tecnológicos

Juan de Dios Bátiz

“Conceptos de Sistemas de Seguridad”

Materia: Seguridad Web y Aplicaciones

Alumno: Jara Hernández Carlos Sebastián

Profesor: Juan Manuel Cruz Mendoza

Grupo: 5IM9

1-SSL(Secure Socket Layer): SSL(Secure Socket Layer), significa (Capa de Socket Seguro), es un protocolo de seguridad utilizado en Internet para garantizar que la información transmitida entre un usuario y un sitio web o entre servidores esté cifrada y protegida.

SSL tiene una capa adicional de seguridad al establecer una conexión segura, lo que impide que terceros, que no estén autorizados puedan leer o manipular los datos durante la transferencia. Este protocolo es muy común utilizarse en transacciones en línea, inicio de sesión en sitios web y otras actividades donde la privacidad y la seguridad son importantes.

2.- Intrusos

Un intruso es una persona que intenta acceder a un sistema informático o una red sin autorización. Los intrusos pueden ser motivados por el robo de información, el vandalismo o el daño.

3-Detección de intrusos: La detección de intrusos es como tener un "cuidador digital" que vigila constantemente la actividad en una red o sistema informático. Este cuidador analiza el tráfico de datos y los registros en busca de comportamientos extraños o patrones que puedan indicar que alguien está intentando acceder de manera no autorizada o realizar acciones maliciosas. Puede reconocer "firmas" conocidas de ataques previos o detectar cambios en el comportamiento normal de la red. Cuando encuentra algo sospechoso, emite alertas para que los administradores tomen medidas de seguridad y protejan el sistema contra posibles amenazas.

4-Gestión de contraseñas: La gestión de contraseñas es como el cuidador personal de tu vida digital. Esto se trata de tomar medidas para asegurarte de que las contraseñas que se utilizan para acceder a tus cuentas en línea sean fuertes y estén resguardadas de manera segura. Esto incluye crear contraseñas que sean difíciles de adivinar, almacenarlas de manera protegida utilizando herramientas como gestores de contraseñas, y seguir reglas específicas, como cambiarlas constantemente.La gestión de contraseñas le enseña a los usuarios sobre las buenas prácticas, como no compartir contraseñas y estar al tanto de posibles amenazas.

Es importante monitorear y revisar regularmente la seguridad de las contraseñas, identificando posibles vulnerabilidades y realizando auditorías para asegurarse de que se cumplan las políticas de seguridad establecidas.

5-Software dañino: El software dañino, se refiere a programas informáticos que han sido creados con el objetivo de causar problemas o daño en una computadora o sistema. Estos programas maliciosos pueden tomar diversas formas y tener objetivos

variados, como robar información, interrumpir el funcionamiento normal de un sistema o comprometer la seguridad de los datos. Por ejemplo virus, gusanos, troyanos, spyware, ransomware.

Por ejemplo, un virus , un virus se propaga al adjuntarse a otros programas, mientras que un gusano puede moverse de un sistema a otro por sí mismo. Los troyanos se disfrazan como programas legítimos pero realizan acciones dañinas en segundo plano, y el ransomware cifra archivos exigiendo un rescate para recuperarlos.

La protección contra el software dañino implica el uso de programas antivirus y prácticas de seguridad informática, como mantener el software actualizado, tener precaución al abrir correos electrónicos desconocidos y evitar hacer clic en enlaces no confiables.

6-Virus: Un "virus" informático es un tipo de software malicioso,este esta diseñado para replicarse y propagarse a través de programas y archivos, con el objetivo de causar daño en un sistema informático. A diferencia de otros tipos de malware, un virus requiere que el usuario ejecute el programa o archivo infectado para activar su código malicioso. Una vez que se activa, el virus puede llevar a cabo diversas acciones perjudiciales, como corromper o destruir archivos, robar información o permitir el acceso no autorizado.

Es importante protegerse contra los virus utilizando software antivirus actualizado y practicando la seguridad informática, como evitar la descarga de software de fuentes que no son confiables y ser cuidadoso al abrir archivos adjuntos o hacer clic en enlaces desconocidos.

7-Antivirus: Un antivirus es un tipo de software que está diseñado para proteger las computadoras y otros dispositivos contra programas maliciosos, especialmente virus informáticos. Funciona escaneando el sistema en busca de posibles amenazas, como virus, gusanos, troyanos y otros tipos de malware. Cuando detecta un archivo o programa infectado, el antivirus toma medidas para eliminar o neutralizar la amenaza, evitando que cause daño al sistema.
Los programas antivirus suelen ofrecer funciones de protección en tiempo real, monitoreando activamente la actividad del sistema para prevenir infecciones antes de que ocurran.

8-Cortafuegos: Un cortafuegos es como un cuidador digital que protege una red informática al controlar y filtrar el tráfico de datos que entran y salen. Su función principal es establecer barreras y reglas para decidir qué información puede pasar y

qué debe ser bloqueada. Es parecido a un filtro, el cortafuegos ayuda a prevenir accesos que no están autorizados y protege contra amenazas externas al examinar y gestionar el flujo de datos.

9-Diseño de cortafuegos: El diseño de cortafuegos, se refiere al proceso de planificación y configuración de un sistema de seguridad informático que utiliza cortafuegos. Esto implica tomar decisiones estratégicas sobre cómo implementar y estructurar estas barreras de protección dentro de una red o sistema. Incluye definir reglas específicas para permitir o bloquear el tráfico de datos, determinar la ubicación óptima de los cortafuegos en la red y establecer políticas de seguridad que reflejen las necesidades y características específicas de la organización.

10-Sistemas de confianza: Los sistemas de confianza, son entornos o infraestructuras en los cuales los participantes, ya sean dispositivos, usuarios o entidades, pueden operar de manera segura y confiable. Estos sistemas están diseñados con el objetivo de establecer un nivel de seguridad y credibilidad, permitiendo que las interacciones y transacciones ocurran con confianza mutua. En un sistema de confianza, se implementan medidas de seguridad, autenticación y autorización para garantizar que solo aquellos que están debidamente verificados y autorizados puedan acceder a recursos o participar en actividades específicas.

Conclusiones del semestre:

El presente semestre en la unidad de aprendizaje de Seguridad Web y Aplicaciones ha sido una experiencia enriquecedora y gratificante. A lo largo de las clases, he experimentado un entorno educativo que ha destacado por su enfoque interactivo y por la metodología única del profesor, que difiere significativamente de la enseñanza tradicional basada solo en libros. Una de las principales fortalezas de este curso ha sido la habilidad del profesor para hacer que las clases sean interactivas y dinámicas. A través de discusiones abiertas y ejercicios prácticos, logró mantener nuestro interés y participación. Esta metodología no solo facilitó la comprensión de conceptos abstractos de seguridad web, sino que también proporcionó una aplicación práctica de estos conocimientos. En comparación con otras experiencias académicas, este curso destacó por su capacidad para proporcionar una comprensión sólida de los fundamentos de la seguridad web sin caer en la monotonía de la enseñanza convencional. La interacción constante y la aplicación práctica de los conocimientos adquiridos han contribuido significativamente a mi comodidad y confianza al abordar los desafíos de seguridad en entornos digitales.

Retroalimentación al profesor Juan Manuel Cruz Mendoza:

Quiero expresar mi aprecio por su dedicación y entusiasmo en la enseñanza de la unidad de aprendizaje de Seguridad Web y Aplicaciones.

En cuanto a las fortalezas, sus clases fueron excepcionales. La forma en que hizo que los conceptos de seguridad web fueran accesibles a través de ejemplos prácticos fue invaluable. La interactividad de las clases realmente contribuyó a mi comprensión y aplicación de los conocimientos adquiridos. Sin embargo, me gustaría proporcionar una sugerencia de mejora. Sería beneficioso para nosotros, como estudiantes, recibir las tareas con anticipación. Esto nos permitiría planificar mejor nuestro tiempo y abordar los desafíos de manera más efectiva. Además, una pequeña ventana de tiempo antes de las entregas podría facilitar la clarificación de dudas sobre las tareas.

En general, quiero enfatizar que valoro enormemente su dedicación y el esfuerzo que pone en sus clases. Se nota claramente que disfruta enseñar y compartir su conocimiento, y eso hace que las clases sean más inspiradoras. Gracias por su arduo trabajo y por proporcionarnos una experiencia educativa valiosa.

Referencias

Cloudflare.com. Recuperado el 5 de diciembre de 2023, de https://www.cloudflare.com/es-es/learning/ssl/what-is-ssl/

Mauricio, O. C., Israel, R. Z., & Patricia, P. R. (2006). Sistemas de Detección de Intrusos (Ids), Seguridad en Internet. Redalyc.org. https://www.redalyc.org/pdf/4026/402640447006.pdf

Comunicación, C. (2023, febrero 28). Qué es un gestor de contraseñas y por qué contar con uno. Grupocibernos.com. https://www.grupocibernos.com/blog/que-es-un-gestor-de-contrasenas

¿Qué es un virus informático? (s/f). Norton.com. Recuperado el 5 de diciembre de 2023, de https://mx.norton.com/blog/malware/what-is-a-computer-virus

IBM documentation. (s. f.). https://www.ibm.com/docs/es/i/7.1?topic=options-firewalls