Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | # 1| Análisis de Vulnerabilidades y Amenazas

Seguridad Informática I

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Casandra Montserrat Ortiz Cortes

FECHA:29/08/2025

Índice

INTRODUCCION

Consiste en llevar a cabo una serie de análisis y pruebas exhaustivas para identificar puertos abiertos, servicios disponibles y vulnerabilidades en los sistemas de información de tu empresa. Combinamos herramientas avanzadas con análisis experto para ofrecer un diagnóstico completo del estado de seguridad.

Con esta información, nuestros especialistas desarrollan un plan de acción detallado para mitigar las amenazas identificadas, fortalecer la infraestructura tecnológica y proteger los activos de tu organización frente a posibles ataques.
Consiste en realizar un análisis profundo y especializado de la seguridad de tus aplicaciones web. Nuestros especialistas simulan escenarios de ataque tanto desde el exterior (como lo haría un actor malicioso), como desde el interior, donde se asume un nivel de acceso autorizado, evaluando riesgos visibles para usuarios, empleados o terceros conectados a tus sistemas.

La Evaluación de Seguridad en Aplicaciones Web es clave para organizaciones que desarrollan o utilizan plataformas digitales, portales de clientes, e-commerce.

DESCRIPCION

La infraestructura de la institución de Veracruz, con sus salones y departamentos y edificios, así como el centro de cómputo y la biblioteca, requiere una evaluación exhaustiva de sus aspectos de seguridad física y lógica, a diferencia de las vulnerabilidades identificadas, como la falta de control de accesos y la deficiencia en instalaciones eléctricas, representan riesgos significativos que podrían ser explotados, poniendo en peligro la seguridad de equipos y datos críticos, estas pueden encontrarse en diferentes niveles: físico, como instalaciones sin control de acceso o equipos, lógico, como sistemas desactualizados, contraseñas débiles o ausencia de copias de seguridad; y humano, derivado de la falta de capacitación o el descuido de los usuarios. son los eventos, intencionales o accidentales, que pueden aprovechar dichas vulnerabilidades para causar un daño. Estas incluyen ataques cibernéticos como malware, phishing o accesos no autorizados, así como amenazas físicas, tales como robos, incendios, desastres naturales o vandalismo.

JUSTIFICACION

Servicios avanzados que replican técnicas reales utilizadas por atacantes para detectar vulnerabilidades críticas en tu infraestructura, aplicaciones y redes. De forma ética, controlada y profesional, nuestros especialistas identifican brechas de seguridad y entregan un informe detallado con recomendaciones técnicas y estratégicas para mitigar los riesgos.
Nuestro servicio de Pruebas de Penetración Móvil ofrece una evaluación integral de la seguridad de las aplicaciones en dispositivos móviles, detectando vulnerabilidades, riesgos y posibles vectores de ataque.

Beneficios clave:
- Evaluación profunda de seguridad.
- Identificación de vulnerabilidades y debilidades.
- Visión clara de vectores de ataque y exposición.
- Protección de datos sensibles y confianza del usuario.

Garantiza la integridad de la información, proteger datos críticos y reforzar la confianza de los usuarios.
Identificar vulnerabilidades de seguridad dentro del ciclo de desarrollo (SDLC). Permite detectar riesgos de forma temprana, reducir costos de corrección y garantizar el cumplimiento normativo, sin necesidad de software adicional.

DESARROLLO

TABLAS DE ANALISIS

Amenazas Humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades De Almacenamiento	Vulnerabilidades De Comunicación
● Los docentes registran su entrada en una libreta y los departamentos utilizan tarjetas de registro . ● No se tiene denegado el uso del equipo para actividades personales, por ejemplo, el acceso a redes sociales o el manejo del correo electrónico o **WhatsApp**. ● Por su parte, el Servidor 2 se destina para alojar un sistema de control que descargaron de Internet, y que les ayuda para mantener los registros de los alumnos (se desconoce la fuente de este software). ● El área administrativa financiera no cuenta con una alarma de seguridad para su acceso.	● El antivirus es nod32 versión gratuita en todos los equipos. ● El firewall no se encuentra habilitado. ● 1 Servicio de internet de 20GB comercial.	● La institución educativa se encuentra en Veracruz ,cerca de la costa. ● Actualmente tiene 4 escaleras de acceso a planta superior y 1 ascensor principal. ● Presenta una entrada principal 2 laterales y posterior a la cancha principal una salida. ● No se identifica dispositivo de detección de sismos, u otros fenómenos naturales. ● Se cuenta con 2 extintores Clase A y uno Clase B ubicados en el piso principal.	● Se cuenta con una salida de emergencia. ● Se cuenta con un servidor principal(diferente al del centro de cómputo). ● 1 servidor espejo. ● 4 equipos por departamento. ● Los equipos han estado lentos en el último mes y se están quedando sin espacio de almacenamiento. ● El Servidor cuenta con la base de datos general. Este utiliza el software Oracle Database en un sistema operativo Linux.	● Los equipos de la planta baja se encuentran conectados por cable de manera directa al módem. Los del piso de arriba son portátiles y se conectan vía wifi. ● 10 equipos de escritorio. ● 5 laptops.

● Su infraestructura es de 2 pisos con 18 salones , 3 departamentos (Contabilidad y finanzas / Dirección / Desarrollo Académico/ , así como un centro de cómputo y una biblioteca.				

CONCLUSION

Un análisis de riesgos y vulnerabilidades es un método para definir, identificar, clasificar y priorizar las debilidades de una aplicación, servicio, organización, etc. Realizar un análisis de riesgos y vulnerabilidades puede ayudar a proteger su organización, sistema o proceso de posibles amenazas.

1. Identificar los activos críticos: Primero, identifique los activos críticos que deben protegerse. Esto podría incluir información confidencial, sistemas de tecnología, edificios.
2. Identificar las amenazas potenciales: A continuación, en su análisis de riesgos y vulnerabilidades, identifique las amenazas potenciales a los activos críticos. Esto podría incluir amenazas físicas como incendios o inundaciones, amenazas cibernéticas como ataques de hackers, y amenazas internas como el robo por parte de empleados.
3. Evalúe la vulnerabilidad de cada activo crítico a cada amenaza identificada.
4. Evaluar el impacto potencial: Evalúe el impacto potencial de cada amenaza en cada activo crítico. ¿Qué tan grave sería el daño si se explotara una vulnerabilidad?

REFERENCIA

ESET Store. (2025, 26 agosto). ***Servicios Ethical Hacking - ESET Store.*** **https://esetstore.com/ethical-hacking/?utm_term=analisis%20de%20vulnerabilidades&utm_campaign=Servicios_Ethical_Hacking&utm_source=adwords&utm_medium=ppc&gad_source=1&gad_campaignid=22874724606&gbraid=0AAAAAC-1m9ZQ-KLby_KjGu6aTEB4NlL03&gclid=CjwKCAjw2brFBhBOEiwAVJX5GOjE3mxYKyjjCqwuxAiR_ChkBvc_Vw-kJsqbqcOvta2UUcTufm1X8RoC2-8QAvD_BwE**