4.8 Herramientas de auditoria

4.8.1 Prueba de penetracion

Una prueba de penetración (también conocida como "pen test" o prueba de intrusión) es un método de evaluación de seguridad de sistemas informáticos que se lleva a cabo para identificar y explotar vulnerabilidades en la seguridad del sistema.

El objetivo de una prueba de penetración es simular un ataque de un hacker o ciberdelincuente para evaluar la efectividad de las medidas de seguridad y para identificar debilidades en el sistema que puedan ser explotadas por personas malintencionadas.

Durante una prueba de penetración, los expertos en seguridad informática utilizan herramientas y técnicas para intentar penetrar en el sistema, realizar actividades maliciosas y, en última instancia, obtener acceso no autorizado a los datos y recursos del sistema.

El resultado de una prueba de penetración es un informe detallado que identifica las vulnerabilidades encontradas, las técnicas utilizadas para explotarlas y las recomendaciones para corregir las fallas de seguridad detectadas. Esto ayuda a las organizaciones a mejorar su seguridad informática y a protegerse contra posibles ataques.

La prueba de penetración ha evolucionado a lo largo de los años junto con el creciente uso de la tecnología y la creciente necesidad de proteger los sistemas informáticos contra los ataques de ciberdelincuentes.

La primera prueba de penetración documentada fue realizada en la década de 1960 por los ingenieros de la compañía Bell Labs. La prueba se llevó a cabo en el sistema operativo Multics para evaluar su seguridad. Desde entonces, las pruebas de penetración se han utilizado cada vez más para identificar vulnerabilidades en los sistemas informáticos y mejorar la seguridad de las organizaciones.

El aumento de los ataques informáticos en la década de 1990 llevó a un mayor enfoque en la seguridad informática y el uso de pruebas de penetración para identificar y corregir las vulnerabilidades. En la década de 2000, la creciente preocupación por la seguridad cibernética en la industria y el gobierno impulsó la demanda de pruebas de penetración y el desarrollo de mejores herramientas y técnicas para llevarlas a cabo.

Hoy en día, las pruebas de penetración son una práctica común en el campo de la seguridad informática y son utilizadas por organizaciones de todos los tamaños para proteger sus sistemas contra los ataques de ciberdelincuentes.

Los pasos de una prueba de penetración pueden variar dependiendo del alcance y la complejidad de la evaluación, pero generalmente siguen los siguientes pasos:

* Planificación: El primer paso en una prueba de penetración es la planificación. Esto incluye establecer los objetivos de la prueba, definir el alcance y determinar los sistemas que serán evaluados.
* Recopilación de información: En este paso, se recopila información sobre los sistemas que se van a evaluar. Esto incluye información sobre los sistemas operativos, aplicaciones, direcciones IP y otras características que puedan ser útiles para identificar vulnerabilidades.
* Análisis de vulnerabilidades: Una vez que se ha recopilado la información necesaria, se realiza un análisis de vulnerabilidades para identificar posibles debilidades en los sistemas. Esto se hace mediante el uso de herramientas automatizadas y técnicas de análisis manual.
* Explotación: Una vez que se han identificado las vulnerabilidades, se intenta explotarlas para obtener acceso no autorizado a los sistemas. Esto se hace mediante el uso de herramientas y técnicas de ataque que simulan los métodos que un atacante real podría utilizar.
* Informe y recomendaciones: Finalmente, se elabora un informe detallado que describe las vulnerabilidades encontradas, las técnicas utilizadas para explotarlas y las recomendaciones para corregir las fallas de seguridad detectadas. Esto ayuda a las organizaciones a mejorar su seguridad informática y a protegerse contra posibles ataques.

Es importante destacar que una prueba de penetración debe ser realizada por profesionales capacitados y con experiencia en el campo de la seguridad informática para garantizar que se sigan los estándares y prácticas adecuadas, y que se evite cualquier daño o interrupción en el sistema evaluado.

No existe una única agencia o entidad que regule las pruebas de penetración a nivel global, pero hay varios organismos y estándares que establecen las mejores prácticas y los requisitos para llevar a cabo pruebas de penetración de manera segura y efectiva. Algunas de estas organizaciones y estándares son:

* PCI Security Standards Council: Este es un organismo que establece los estándares de seguridad para la industria de pagos en línea y requiere pruebas de penetración regulares como parte del proceso de cumplimiento de PCI.
* National Institute of Standards and Technology (NIST): Esta es una agencia gubernamental de los Estados Unidos que establece los estándares para la seguridad informática y proporciona directrices para la realización de pruebas de penetración.
* ISO/IEC 27001: Este es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) y proporciona orientación sobre la realización de pruebas de penetración.
* Open Web Application Security Project (OWASP): Es una organización que proporciona recursos y herramientas para mejorar la seguridad de las aplicaciones web y que tiene un proyecto específico sobre pruebas de penetración.

Además, algunos países tienen leyes y regulaciones específicas en relación con las pruebas de penetración. Por lo tanto, es importante consultar con expertos en seguridad informática y asesores legales para garantizar que se cumplan todos los requisitos legales y normativos aplicables antes de llevar a cabo una prueba de penetración.

El salario de un profesional que se dedica a hacer pruebas de penetración (pentesting) puede variar significativamente dependiendo de varios factores, como la experiencia, la ubicación geográfica, la industria y el tamaño de la empresa para la que trabaja.

Según información de Glassdoor, el salario base promedio de un especialista en seguridad cibernética en los Estados Unidos es de alrededor de $100,000 al año, mientras que un consultor de seguridad cibernética puede ganar un promedio de $120,000 al año.

Sin embargo, algunos profesionales de seguridad cibernética especializados en pentesting pueden ganar aún más, especialmente si tienen habilidades muy específicas y avanzadas. En algunos casos, los profesionales con experiencia y habilidades especializadas pueden cobrar más de $200 por hora por realizar pruebas de pentesting.

Es importante destacar que el salario y la compensación de los profesionales de la seguridad cibernética dependen de muchos factores y puede variar significativamente de una región a otra y de una empresa a otra. Por lo tanto, es importante investigar y comparar las ofertas de trabajo y los salarios en la industria de seguridad cibernética para obtener una idea más precisa de lo que puede ganar un especialista en pentesting.

La multa por vulnerar un sistema sin permiso varía según la legislación de cada país y la gravedad del delito cometido. En general, la ley considera la vulneración de sistemas informáticos sin permiso como un delito y puede ser sancionado con multas y/o penas de prisión, dependiendo de la jurisdicción y la naturaleza del delito.

En los Estados Unidos, por ejemplo, la Ley de Fraude y Abuso Informático (CFAA) establece penas que van desde multas de hasta $250,000 y penas de prisión de hasta 5 años por la primera ofensa, y penas más severas para delitos más graves o reincidentes. Además, las empresas o individuos afectados por una vulneración de seguridad pueden presentar demandas civiles para recuperar daños y perjuicios.

En otros países, las multas y las penas pueden ser diferentes y variar según la legislación local. Por lo tanto, es importante conocer las leyes y regulaciones locales y nacionales en relación con la vulneración de sistemas informáticos sin permiso y los posibles castigos que se pueden imponer.

En cualquier caso, vulnerar un sistema sin permiso es ilegal y puede tener graves consecuencias legales, financieras y de reputación. Siempre es recomendable obtener permiso explícito y por escrito antes de llevar a cabo cualquier prueba de penetración o evaluación de seguridad informática.

4.8.2 Hacking ético

El hacking ético (también conocido como "pruebas de penetración" o "pen testing") es una práctica de seguridad informática en la que un profesional de seguridad informática utiliza técnicas de hacking para identificar y explotar vulnerabilidades en sistemas y aplicaciones con el objetivo de evaluar su seguridad y mejorarla.

A diferencia del hacking malicioso, que tiene como objetivo dañar o robar información, el hacking ético se lleva a cabo con el consentimiento del propietario del sistema o aplicación y se realiza para mejorar la seguridad del mismo. Los hackers éticos pueden trabajar para empresas de seguridad informática, consultoras de seguridad o incluso para la propia organización que desea evaluar la seguridad de su sistema.

El hacking ético implica la realización de pruebas de seguridad para identificar posibles vulnerabilidades, analizar los resultados y proporcionar recomendaciones para mejorar la seguridad del sistema. Estas pruebas pueden incluir técnicas como el escaneo de puertos, la identificación de vulnerabilidades de software, el uso de herramientas de explotación, la realización de pruebas de inyección de código, entre otras.

El objetivo final del hacking ético es mejorar la seguridad del sistema y garantizar que los datos de la organización estén protegidos contra posibles ataques cibernéticos.

Aunque los pasos específicos del hacking ético pueden variar según la metodología utilizada, a continuación se presentan algunos de los pasos comunes que se suelen seguir durante un proceso de pruebas de penetración:

Recopilación de información: En este paso, se recopila información sobre el sistema o aplicación objetivo, incluyendo información sobre su arquitectura, tecnologías utilizadas, permisos de acceso, entre otros.

Análisis de vulnerabilidades: En este paso, se utiliza software especializado para identificar vulnerabilidades en el sistema o aplicación objetivo. Esto puede incluir el uso de herramientas de escaneo de puertos, análisis de vulnerabilidades de software, entre otros.

Explotación de vulnerabilidades: Una vez que se han identificado las vulnerabilidades, se lleva a cabo un intento de explotación de las mismas. Esto puede implicar la realización de pruebas de inyección de código, el uso de herramientas de explotación, o la realización de ingeniería social.

Acceso y control del sistema: Si se logra explotar con éxito una vulnerabilidad, el siguiente paso es obtener acceso y control del sistema. Esto puede incluir la obtención de credenciales de inicio de sesión, la elevación de privilegios, entre otros.

Mantenimiento del acceso: Una vez que se ha obtenido acceso al sistema, el objetivo es mantener el acceso a largo plazo. Esto implica la creación de backdoors, la modificación de permisos y configuraciones, entre otros.

Informe de resultados: Por último, se elabora un informe detallado que incluye las vulnerabilidades encontradas, el grado de riesgo de cada una, las recomendaciones para solucionarlas, y cualquier otra información relevante. Este informe se presenta al propietario del sistema o aplicación para que pueda tomar medidas para corregir las vulnerabilidades identificadas.

Es importante destacar que estos pasos pueden variar dependiendo de la metodología de hacking ético utilizada, pero en general, estos son los pasos que se suelen seguir para llevar a cabo pruebas de penetración.

El hacking ético es importante por varias razones:

Mejora la seguridad: Las pruebas de penetración permiten identificar vulnerabilidades en sistemas y aplicaciones antes de que puedan ser explotadas por hackers malintencionados. Al corregir estas vulnerabilidades, se puede mejorar significativamente la seguridad del sistema.

Ahorra costos: Las pruebas de penetración son una inversión rentable ya que pueden ahorrar costos significativos al prevenir pérdidas de datos o interrupciones en el servicio que podrían tener consecuencias económicas negativas.

Cumplimiento de regulaciones: Muchas industrias están reguladas y requieren pruebas de seguridad para garantizar el cumplimiento de las normas de seguridad y privacidad de los datos. Las pruebas de penetración son una forma efectiva de cumplir con estos requisitos.

Protección de la reputación: Una brecha de seguridad puede afectar la reputación de una organización. Las pruebas de penetración pueden ayudar a prevenir estas situaciones al mejorar la seguridad de los sistemas y reducir el riesgo de violaciones de seguridad.

Mantenimiento del liderazgo del mercado: Una organización que demuestra un enfoque proactivo hacia la seguridad y la privacidad de los datos puede tener una ventaja competitiva y mantener su liderazgo en el mercado.

En resumen, el hacking ético es importante porque ayuda a proteger los sistemas y datos de las organizaciones, a reducir costos y a garantizar el cumplimiento de las regulaciones de seguridad y privacidad de los datos. Además, puede ayudar a proteger la reputación de una organización y mantener su liderazgo en el mercado.