Servicio de Análisis de Vulnerabilidades y Pentesting persistente

Módulo Análisis de Vulnerabilidades Persistente

Descripción

Deberá analizar los activos informados de forma automática con el fin de identificar vulnerabilidades potenciales en los sistemas de información y descubrir nuevos sistemas, identificar puertos abiertos e incluso comprobar si la configuración de los mismos cumple con los estándares de seguridad.

En una primera fase se definirán el conjunto de sistemas, redes y plataformas críticas que formarán parte del alcance del módulo. Unido a ello, se acordarán y planificarán con el proveedor las ejecuciones de los análisis, las franjas horarias, la periodicidad de las pruebas, las posibles restricciones y las políticas de escaneo (pruebas a realizar).

En base a la información acordada el proveedor se encargará de realizar la configuración de las herramientas e iniciar la ejecución del proceso de análisis de vulnerabilidades. Es recomendable que el equipo de trabajo realice un escaneo de descubrimiento inicial. Este proceso no requiere de la instalación de hardware ni software adicional y no precisa de tareas de configuración.

Cuando la ejecución de las pruebas hayan finalizado, los resultados de los análisis deberán ser cargados automáticamente en el Portal del Servicio. Se deberá poder generar de forma ilimitada informes técnicos, de seguimiento y diferenciales que le permitan ver la evolución del servicio.

Módulo de Pentesting Persistente

Descripción

El pentesting no solo detecta las brechas en la seguridad o sus correspondientes vulnerabilidades, sino que las explota. Muestra las posibles formas de acceso a una compañía, haciéndonos pasar por ciberdelincuentes para así poder corregir las brechas encontradas y explotadas.

Fases de un pentesting

- Reconocimiento
- Análisis de vulnerabilidades
- Explotación
- Post explotación
- Informes

Fase de Reconocimiento

En esta fase existen dos modalidades: pasivo y activo. En el reconocimiento pasivo la información se consigue sin interacción directa con el objetivo mediante el uso de técnicas tales como la ingeniería social, búsquedas por internet (realizando consultas a DNS, Shodan, etc). Por otra parte el reconocimiento activo comprende un estudio de la red para descubrir equipos individuales, direcciones IP y los servicios expuestos.

Realizando ambos reconocimientos, el pasivo y el activo, se consigue información útil para llevar a cabo el ataque. Esta información facilita descubrir algunas vulnerabilidades de los sistemas que gestionan y protegen la información.

Fase de Análisis de vulnerabilidades

El análisis de vulnerabilidades tiene como objetivo evaluar las debilidades que puedan existir en un determinado software, aplicación o sistema que pudiera afectar a su integridad.

A partir de la información obtenida en la fase anterior se intenta identificar vulnerabilidades ya conocidas sobre los sistemas y aplicaciones. Como resultado se obtiene un informe detallado de las vulnerabilidades encontradas.

Simultáneamente se combinan técnicas propias de un ciberdelincuente simulando un ataque real en función de lo recopilado en la fase de reconocimiento.

Fase de Explotación

La fase de explotación consiste en realizar todas aquellas acciones que puedan comprometer al sistema auditado, a los usuarios o a la información que maneja.

Principalmente se comprueba que no se puedan realizar ataques tipo:

- Inyección de código
- Inclusión de ficheros locales o remotos
- Evasión de autenticación
- Carencia de controles de autorización
- Ejecución de comandos en el lado del servidor
- Ataques tipo Cross Site Request Forgery
- Control de errores
- Gestión de sesiones
- Fugas de información
- Secuestros de sesión
- Comprobación de las condiciones para realizar una denegación de servicio
- Carga de ficheros maliciosos

Estos tipos de ataques se realizan adecuando el desarrollo de cada ataque, técnicas en uso y las últimas tecnologías disponibles adaptadas para conseguirlo.

Post explotación

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta.

En función de las posibilidades que permita una vulnerabilidad concreta, se intentarán realizar las siguientes acciones de post explotación:

- Obtención de información confidencial
- Evasión de mecanismos de autenticación

- Realizar acciones del lado de los usuarios
- Realizar acciones o ejecutar comandos en el servidor que aloja la aplicación
- Privilegios disponibles en el servidor, si se consigue acceso al mismo
- Otros sistemas o servicios accesibles desde la aplicación comprometida
- Posibilidad de impersonalización del usuario
- Realizar acciones sin el consentimiento o conocimiento de los usuarios

La posibilidad de encadenar varias vulnerabilidades para conseguir un acceso de mayor nivel o para evadir los controles de seguridad también serán escenarios valorados a la hora de realizar el análisis de riesgos.

Informes

La última parte de un test de intrusión es realizar un resumen informativo donde se incluirán todas las vulnerabilidades encontradas y las exposiciones que podrían aprovechar los atacantes.

También se debe incluir un documento donde se recopile todo lo obtenido en la prueba. Podemos considerarlo una muestra de la información que podría haber sido recopilada por un atacante.

Por último, debe constar, un documento de contra medidas para resolver (o mitigar) en medida de lo posible estos problemas.

Definición del alcance del servicio de Escaneo de vulnerabilidades

El servicio deberá cubrir lo expuesto anteriormente aplicado sobre un máximo de 50 activos expuestos a internet mediante un máximo de 40 IP públicas. Por razones de seguridad, el detalle de los activos, IPs y URLs será entregado al prestador del servicio una vez perfeccionada la Orden de Compra/Provisión correspondiente y firmado por las partes, el Acuerdo de Confidencialidad que se anexa a estas especificaciones técnicas. Asimismo se detallará las bandas horarias y días en que se deberán realizar los análisis de forma de no afectar las labores de los agentes del Ministerio Pùblico.