



Servicio de Pentesting Avanzado

Conoce nuestra herramienta de detección de vulnerabilidades

A través de Penthor, analizamos pruebas de penetración (pentesting) que ayudan a descubrir las vulnerabilidades de tu red, llevando a cabo ataques basados en exploits en condiciones reales y sin interrupción del servicio

Un servicio completo con las mejores características

- **DESATENDIDO:** las pruebas de intrusión comienzan con acceso físico a la LAN sin credenciales, igual a cómo operan los hackers
- **EXPLOITS INOFENSIVOS:** realizamos ataques de vulnerabilidad como si de un hacker se tratara, pero sin interrumpir el servicio
- **AUTOMATIZADO:** desde Excem nos encargamos del servicio de forma transparente para el cliente.
- **REMIEDIACIÓN PRIORIZADA:** obtén un resumen detallado de los críticos a seguir para remediar en función de las prioridades de amenazas para tu empresa.
- **ÚLTIMAS TÉCNICAS DE HACKING:** ponemos a tu disposición las técnicas de pentesting más actualizadas del mercado.
- **ALERTAS PERSONALIZADAS:** establece objetivos de pruebas de intrusión y ejecutar una prueba de ataque dirigida a una vulnerabilidad concreta.

Beneficios



PROTECCIÓN CONTINUA

Prueba toda tu infraestructura con una amplia gama de técnicas de hacking para garantizar que siga siendo resistente, independientemente de cómo el hacker intente entrar



DEFENSA ACTUALIZADA

Mantente al día con las últimas técnicas de hacking. Nuestra herramienta proporciona las técnicas de pentest más recientes en profundidad.



VALIDACIÓN CONSTANTE

Realiza lost tests configurándolos con la periodicidad que desees.



DESPLIEGUE FÁCIL

Se instala localmente en tu red para proteger de manera efectiva sus vulnerabilidades de internet y del exterior. Transparente para el cliente, ya que su instalación corre a cargo de nuestro equipo técnico.

EXCEM
TECHNOLOGIES

PENTHOR

AS
Ajoomal Services

La solución de Excem está diseñada poniendo por delante las necesidades del personal técnico (administradores de sistemas y personal de ciberseguridad) y ofreciendo la parte administrativa que se espera de estas soluciones de cara a cumplimiento normativo.

Se tienen en cuenta las posibles necesidades del usuario y, en vez de requerir la instalación de agentes o de una máquina potente, se puede realizar el despliegue local de una sonda que conectará de forma segura con la máquina de procesamiento que realizará todo el trabajo. El despliegue de la sonda es trivial, necesitando tan solo un sistema capaz de conectar por VPN, la empresa ofrece soluciones físicas (Raspberry Pi o similar que el cliente solo tiene que conectar) y lógicas de diferentes tipos (imágenes para Raspberry o VM compatibles con VMWare). En casos especiales también puede instalarse en local.

- Despliegue mediante contenedores para facilitar la actualización de cada módulo, el despliegue y la localización y solución de problemas.
- Diferentes roles de personal con acceso a la solución para adecuarlo a las necesidades del cliente.
- Módulos de análisis de vulnerabilidades y exploits con capacidad para realizar las técnicas de MSF y parte de las de Kali Linux.
- Alta velocidad para ataques de enumeración de sistemas y servicios.
- Velocidad media para ataques de análisis de vulnerabilidades y pentesting.
- Informes interactivos disponibles para el usuario.
- Interfaz multi-tenant en el servidor.
- Informes ejecutivos, detallados, por host, vulnerabilidad tanto en PDF como en XLS.
- Aprendizaje entre ejercicios.
- Capacidad de solucionar problemas en el sistema al vuelo al ser una solución propia.
- Interfaz en español, inglés y portugués
- Bajo impacto en las instalaciones del cliente.
- Dashboard con resumen del ejercicio en la interfaz.