COEUS CYBERSECURITY

PENTEST

Prueba de Penetracion Controlada

COEUS CYBERSECURITY

Un Pentest es una simulacion controlada de un ataque cibernético realizada por expertos autorizados. Su objetivo es identificar vulnerabilidades reales antes de que un atacante malicioso las explote.

AUTORIZADO **CONTROLADO** **CONFIDENCIAL**

Por que realizarlo?

Prevenir ataques
Detecta fallos antes que los hackers.

Cumplimiento legal
ISO27001,PCI-DSS, NIST, GDPR

Reducir riesgo
Protege datos,clientes y reputacion.

Las 5 Fases del Pentest

1 Reconocimiento
Recoleccion de informacion publica: IPs, dominios, tecnologias y empleados clave.
Objetivo: mapear la superficie de ataque

2 Escaneo
Identificacion de puertos abiertos, servicios activos y configuraciones debiles.
Herramientas: Nmap, Nessus, OpenVAS

3 Explotacion
Aprovechamiento controlado de vulnerabilidades para obtener acceso al sistema.
Objetivo: validar el impacto real del fallo

4 Post-Explotacion
Evaluacion del alcance del acceso: datos expuestos, escalacion de privilegios.
Objetivo: medir el dano potencial

5 Reporte
Entrega de informe tecnico-ejecutivo con hallazgos, riesgos y plan de remediacion.
Resultado: hoja de ruta para corregir

Tipos de Pentest

Sin info previa. Simula un atacante externo.	Acceso total al sistema. Maxima cobertura.	Informacion parcial. Combina perspectivas.	Ataque multi-vector. Prueba defensa total.

Protege tu empresa con COEUS Cybersecurity

Expertos en seguridad ofensiva y pentesting en Ciudad de Mexico

www.coeus.com.mx ping@coeus.com.mx CDMX, Mexico

coeus