KEY

SERVICIOS PENTESTING

2019

PENTESTING

Los riesgos actuales asociados a Internet. Ciberriesgos.

ciberriesgos inherentes a la actividad empresarial.

- Cualquier IP pública de nuestras infraestructuras de red y/o sistemas es una puerta expuesta en Internet que debe contar con las adecuadas medidas de seguridad y protección.
- Cualquier vulnerabilidad de este elemento queda expuesta a Internet y por lo tanto es susceptible de ser identificada y utilizada para realizar un ataque.
- Podemos establecer dos tipologías de vulnerabilidades asociadas a los elementos que exponemos a Internet:
  - **Entornos Web y aplicaciones.** Técnicas de SQL Inyection, Cross-Site Scripting (XSS), Buffer Overflow, Authentication Bypass o File Inclusion son errores de programación conocidos y utilizados por los hackers.
  - **Infraestructuras.** Revelación de información, insuficiente nivel de parcheado, credenciales débiles, certificados digitales expirados, insuficiente medidas de protección como IPS y FWs, una mala segmentación de red y/o mala arquitectura de sistemas hacen posible un ataque con éxito desde el exterior.

- **El hacking se "democratiza".** Existen múltiples herramientas en Internet como SQLmap o Hajiv. Se trata de herramientas amigables que permiten a cualquiera (sin conocimientos en bases de datos, SQL o técnicas de hacking) explotar este tipo de fallos.

PENTESTING

El HE es una excelente herramienta para calibrar con precisión los ciberriesgos:

- **Sus principales capacidades al servicio de la Ciberseguridad son:**
  - Auditoría a distancia de entornos complejos en cualquier ubicación.
  - Identificar e inventariar las vulnerabilidades asociadas a cada elemento de red y/o sistema.
  - Identificar los vectores de ataque más factibles y analizarlos para calibrar el riesgo real que suponen para la compañía.
  - Identificar qué activos están expuestos a internet y tomar las correspondientes evidencias.
  - Hacer un seguimiento ágil y eficiente de los planes de remediación al permitir un retesting inmediato para verificar la efectividad de las medidas correctivas adoptadas.
  - Análisis forenses detallados para calibrar el daño/alcance real de una infiltración e identificar los vectores de ataque utilizados.

- **Otras capacidades adicionales. Alerta temprana (Ciberinteligencia):**
  - Identificación proactiva de amenazas y ataques de Zero-Day.
  - Seguimiento, investigación e infiltración en los foros “underground” para:
    - Identificar robos de información o acciones dolosas contra la compañía.
    - Establecer mecanismos de alerta temprana para prevenir/gestionar con antelación ataques de hacktivismo.

PENTESTING

¿Cómo lo hacemos?

Aplicamos dos esquemas de trabajo divididos en dos etapas:

- **Fase 1. Pentest de Caja Negra.**
  - Este trabajo se realiza exclusivamente desde Internet para calibrar con precisión nuestro nivel de exposición o ciberriesgo externo.
  - Se hace un inventario del equipamiento visible desde internet y se identifican sus vulnerabilidades.
  - Se aplican técnicas de HE a los vectores de ataque identificados como más factibles y se obtienen evidencias de los resultados.

- **Fase 2. Pentest de Caja Blanca.**
  - Este trabajo se realiza desde dentro de la red y es un complemento fundamental a la Fase 1 ya que una vez roto el perímetro exterior los hackers aprovechan las vulnerabilidades internas para profundizar en sus ataques.
  - Se analiza el diseño de seguridad de la topología de la red y la arquitectura de los sistemas.
  - Se audita el bastionado de los elementos críticos.
  - Se verifica el nivel de resistencia frente ataques internos y externos. Un empleado desleal (insider) puede ser muy peligroso debido al conocimiento detallado que puede tener de los datos de la compañía.

Para la realización de estos trabajos **se utilizan herramientas especializadas debidamente parametrizadas que se complementan con otras diseñadas por la compañía** para este tipo de actividades. **Nuestra metodología tiene una componente manual,** para garantizar un inventario muy preciso de las vulnerabilidades y su riesgos reales para la organización que con herramientas automáticas es imposible alcanzar.

PENTESTING

A la hora de identificar las vulnerabilidades y calibrar los riesgos se aplican estándares internacionalmente reconocidos:

- **OSSTMM. Open Source Security Testing Methodology Manual.**
- Es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet.
- Incluye un marco de trabajo que describe las fases que habría de realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre cientos de expertos internacionales sobre el tema, que colaboran entre sí mediante Internet.

http://osstmm.org

- **CVSS. Common Vulnerability Scoring System.**
- Con el objetivo de valorar de forma objetiva las vulnerabilidades utilizamos la metodología CVSS que es el estándar internacional de facto.
- La elección de esta métrica se basa en la necesidad de tener un sistema de valoración independiente de los fabricantes y respaldada por un organismo de referencia a nivel mundial como el FIRST

http://first.org/cvss/

PENTESTING

Criterios de valoración de vulnerabilidades del estándar CVSS:

NIVEL DE RIESGO	AMENAZA
Bajo	Se consigue información pública de la compañía, pero que supone un daño mínimo o nulo al negocio; o bien se consigue información sobre el sistema analizado pero no se consigue utilizarla para explotar nuevas vulnerabilidades.
Medio	Se consigue información sensible de la compañía: información financiera básica (facturaciones, beneficios), detalles de proyectos, información básica sobre clientes (nombres y etc.), datos de carácter personal de nivel bajo (nombre, apellidos, direcciones de contacto, teléfonos, números de Cuentas corrientes).
Alto	Acceso a datos de carácter privado: historiales de trabajo (Curriculum Vitae, datos de la Seguridad Social), datos de carácter personal de nivel medio (datos relativos a infracciones administrativas o penales, de hacienda pública, servicios financieros, solvencia patrimonial o crédito); o bien se logra explotar una vulnerabilidad que permite ejecución de comandos o shell directamente en la máquina como usuario; obtención de credenciales de acceso a sistemas, bases de datos o aplicaciones; acceso masivo a datos de la base de datos.
Crítico	Acceso a datos de carácter confidencial: secretos comerciales, datos de carácter personal de nivel alto (ideología, religión, creencias, origen racial, salud, vida sexual, datos con fines policiales sin consentimiento del interesado), código fuente de aplicaciones, información útil para la competencia; o bien se consigue ejecución de comandos o Shell como usuario de administración del sistema.

PENTESTING

Para soportar nuestras recomendaciones aplicamos igualmente dos estándares internacionales:

- **OWASP. Open Web Application Security Project.**
- La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo.
- Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.
- Estar libre de presiones corporativas facilita que OWASP proporcione información imparcial, práctica y reutilizable sobre seguridad de aplicaciones informáticas.

http://owasp.org

- **CIS. Center for Internet Security.**
- Es una organización sin ánimo de lucro cuya misión principal es mejorar los niveles de ciberseguridad y la capacidad de respuesta a los ciberriesgos de las entidades públicas y privadas. Entre sus miembros se encuentra el US Departament of Homeland Security.
- Posee una de la más amplia, reputada y mejor contrastada biblioteca de guías técnicas de bastionado.

http://cissecurity.org

CENTER FOR INTERNET SECURITY

PENTESTING

Desarrollamos nuestras propias herramientas

Disponemos de una plataforma para la realización de los test de penetración a distancia de nuestros clientes y el seguimiento de su nivel de ciberriesgo. La plataforma está compuesta de 3 componentes principales:

- **Plataforma de Pentest.**
  - Está optimizada para la realización de Pentest de forma ágil y segura ya que está optimizada para aplicar nuestra propia metodología desarrollada durante años.
  - Permite realizar retesting de forma inmediata para verificar el resultado de los planes de remediación.
  - Permite la programación de nuevos test de penetración, totales o parciales, para la calibrar la evolución del nivel de ciberriesgo del cliente.
- **Sondas de HE.**
  - Se trata de una sonda basada en tecnología Raspberry con sistema operativo NetBSD fuertemente hardenizado que actúa como Gateway seguro para la realización remota de test de caja blanca.
  - Al ser pequeña y muy fácil de instalar, solo hay que conectarla al segmento de red a auditar, el cliente puede tenerla guardada en un cajón y conectarla en la ventada acordada para la realización de los pentest.
  - Una vez conectada a la red, la sonda establece un túnel seguro con nuestra plataforma.
  - Toda la actividad realizada por la sonda genera un log seguro de actividad que está a disposición del cliente para efectos de trazabilidad y auditabilidad si así lo requiere.
- **Plataforma de Ciberinteligencia.**
  - Elevadas capacidades de búsqueda profunda en Internet para identificar contenidos/informaciones pertenecientes a la compañía (identificación de fugas de información).
  - Posibilidad de hacer seguimiento en determinados foros y redes underground para prevenir e identificar acciones maliciosas contra la compañía.

CONTACTO

MIGUEL BEASCOA

TLF: +51 943 192 231
mail: miguel.beascoa@key-identification.com