Taller de Administración de Servidores Linux

CC5308

Clase 35: 7 de Junio de 2011

Estrategias de Mitigación

Luis León Cárdenas Graide
lcardena [at] nic . cl

Riesgo Inevitable

- Hay amenazas de seguridad que finalmente impactan
- Siempre: Riesgo > 0
- Mitigación: ¿Cómo minimizar el daño?
- Seguridad táctica: amenaza específica
  - ¿Variaciones en ataques?
  - ¿Amenazas desconocidas?
- Seguridad estratégica: transversal y eficiente
  - ¿Amenazas desconocidas?
    - Fundamentalmente insalvables
    - Seguridad Estratégica ayuda ante clases de ataques

Mínimo Privilegio

- Granularidad del objeto protegido
  - Usuario (Rol, puede ser otro subsistema)
  - Componente del sistema
  - Proceso y Tipo de operación
    - Cantidades, plazos, frecuencias, volúmenes, carga
- Requerimientos funcionales inter-procesos
- Servicios asociados a Perfil de Usuario
  - Por diseño, requiere definir casos de uso y roles
- Crecimiento del Sisterma
  - Mantención y nuevos privilegios
- Delegación de privilegios, no credenciales

Defensa en Profundidad

- "Seguridad por capas"
  - Mejor: Cada capa asegurada
- Varias exclusas de seguridad
  - Si falla alguna, todavía hay otras que resistan ataque
- Overlap de protección
- Problemas: si se hace desordenadamente
  - Configuración coherente
  - Mantención
  - Acoplamiento de capas
  - Auto-DoS

Punto de Ahogo

- Concentración de esfuerzos de monitoreo
- Conexiones entrantes y salientes
- SPoF: No reemplaza Defensa en Profundidad
- Performance: Según capa y tipo de transacción
- Típico: Firewall
  - También aplica en otras capas
  - Puede elegirse ahogar una y no otra (o menos)
- Bypass por capas
- Mantención: Concentración de Configuración

Eslabón más débil

- Más fácil de atacar/fallar
  - Evaluar rentabilidad del atacante
  - Candidato a ser reforzado
    - Requiere identificar activos (BCP)
    - Priorización según costo-riesgo-efectividad
    - máx(Vulnerabilidad) != máx(Riesgo)
      - Probabilidad e Impacto
- En cada capa puede haber el suyo
- Debilidades sistémicas intercapas

Estado fail-safe

- Security by default
- ¿Se puede cumplir expectativa/oferta de seguridad si no se cumplen pre-requisitos de seguridad?
- Default: deny vs allow
  - Etapa de pruebas: Allow + Warning
  - En producción: Deny + Monitoreo + Alerta
  - Ojo: Auto-DoS
- Falla de Seguridad ¿!=? Falla Aplicación
  - Requerimiento incumplido

Protección Universal

- Todos los nodos
  - Servidores
  - Conmutadores
  - Estaciones de trabajo y terminales
    - ¿Smartphones?
- Todas las aplicaciones
  - Servidores y Desktop
- Evita dispersar esfuerzos al reaccionar
- ¿Quién lo gestiona? ¿Quién responde?
  - Usuario vs Sysadmin
  - Automático, Remoto

Defensa Diversa

- Monocultivo: Una vulnerabilidad compromete a todo el sistema
- Múltiples Proveedores para el mismo Servicio
- Mantención: Complejidad y Costo
  - Dominio de varios sistemas
- Coexistencia: Interoperatividad y Estandarización
  - ¿Protocolos y Formatos cerrados?
- Diversidad de personal
  - Distintos administradores sobre distintos servicios
  - Errores sistemáticos y compromiso

Simplicidad

- KISS: Keep It Shallow and Simple
- Seguridad demostrable
  - Requiere poder ser analizado
    - Requiere ser simple
- Hacer poco y hacerlo bien
- Mínima Sorpresa

Restricción de Origen/Destino

- ¿Quién realiza la transacción?
  - Es más que simplemente la conexión
  - Depende de cada capa
- ¿A quién se autoriza uso de infraestructura?
- Ver: Punto de Ahogo
- ¿Terminales vulnerables?
  - Origen vs Intención: Phishing vs Rootkit
  - ¿Perímetro? ¿Exterior vs Interior?
    - VPN, Smartphones
- Servicios inutilizados: Necesario vs Innecesario
  - Levantar/instalar vs Bajar/desinstalar

¿Seguridad por Oscuridad?

- Temporalidad de Secretos
  - Requerir secretos breves
  - Proteger muy bien secretos prolongados
- Kirchoff: Clave vs Algoritmo/Diseño
  - ¿Hace falta conocer detalles de sistema vulnerable para atacarlo?
  - ¿Es difícil atacar sistema vulnerable a pesar de no conocer detalles?
  - Ocultar diseño, ¿hace más difícil el ataque? ¿cuánto?
  - ¿Cuánto se pierde por ocultar diseño?
- Mal opuesto: exhibicionismo

Actividad Personal

- ¿Qué servicios tienes corriendo?
- ¿Qué hace / para qué sirve cada uno?
- ¿Qué entradas ofrecen al sistema?
- ¿Qué permiten hacer una vez adentro?
- Desinstalar/bajar superfluos hasta minimal
- Crear distribución que instale minimal