Resumen tema 3 seguridad

**Página 1: Introducción a la Seguridad Perimetral**

* **Definición y concepto**:
  + El perímetro de una red se refiere a los sistemas que conectan la red interna con la externa (generalmente Internet).
  + Dado que están abiertos al exterior, estos sistemas son vulnerables a ataques si no se protegen adecuadamente.
  + La seguridad perimetral consiste en implementar dispositivos y políticas para gestionar qué tráfico entra o sale de la red interna, asegurando un funcionamiento óptimo.
* **Objetivo**:
  + Proteger los recursos internos permitiendo o denegando accesos de usuarios internos y externos.

**Página 2: Redes Sin Seguridad Perimetral**

* **Características de redes sin perímetro de seguridad**:
  + **Red plana sin segmentación**: Si un nodo es comprometido, se accede fácilmente a toda la red.
  + **Exposición de servicios internos**: Sin un cortafuegos, los servicios internos están directamente accesibles desde el exterior.
  + **Falta de monitorización**: No existen sistemas que registren o detecten actividad anómala.
  + **Ausencia de filtrado de tráfico**: El tráfico no es controlado, tanto de entrada como de salida.
  + **Sin verificación de malware o spam**: La seguridad depende únicamente del usuario final.

**Página 3: Funciones de la Red Perimetral**

* Las redes perimetrales se diseñan para:
  1. **Rechazar accesos externos no autorizados** a servicios internos sensibles.
  2. **Discriminar el tráfico interno y externo**, aplicando políticas específicas a cada tipo.
  3. **Seleccionar nodos autorizados**: Permitir tráfico solo entre nodos específicos.
  4. **Centralizar el punto de conexión externa**, facilitando su control.
  5. **Ocultar servicios vulnerables** para evitar que sean identificados o atacados desde el exterior.
  6. **Proteger información interna** (nombres de sistemas, topología de red, cuentas de usuario).

**Página 4-5: Conceptos Clave**

* **Perímetro**:
  + La “frontera” fortificada de la red que incluye dispositivos como routers, cortafuegos, IDS, VPN y redes DMZ.
* **Bastión**:
  + Un servidor o equipo que publica servicios hacia el exterior; diseñado para resistir ataques gracias a su fortificación.
* **Hardening**:
  + Proceso de asegurar y fortificar un servidor, minimizando vulnerabilidades.
* **Cortafuegos**:
  + Dispositivo de seguridad configurado para aceptar o denegar tráfico basado en reglas específicas.
* **IDS (Sistema de detección de intrusos)**:
  + Detecta ataques mediante patrones de información (firmas) o secuencias anómalas de acciones.
* **VPN (Red privada virtual)**:
  + Crea conexiones cifradas a través de redes públicas, proporcionando privacidad y seguridad.
* **DMZ (Zona Desmilitarizada)**:
  + Porción de red donde se alojan servicios públicos (como servidores web) para minimizar riesgos a la red interna.

**Página 6: Defensa en Profundidad**

* **Estrategia**:
  + Implementar múltiples capas de seguridad para reducir la probabilidad de compromiso.
  + Si una capa falla, otras aseguran que el impacto sea mínimo.

**Página 7: Objetivos de la Seguridad Perimetral**

1. **Estabilidad de la red**:
   * Proteger la infraestructura frente a amenazas derivadas de interacciones inseguras de usuarios con Internet.
2. **Navegación segura**:
   * Controlar sitios permitidos mediante listas blancas y negras, además de usar sistemas de reputación.
3. **Optimización de recursos**:
   * Garantizar el uso eficiente de la capacidad de la red.
4. **Detección de malware**:
   * Identificar rápidamente amenazas como virus y programas maliciosos.
5. **Facilidad de conexiones remotas**:
   * Proveer acceso seguro mediante VPN para empleados o sucursales.

**Página 8-9: Arquitecturas de Seguridad**

* **Arquitectura débil**:
  + DMZ ubicada detrás de un único cortafuegos con múltiples interfaces.
  + Riesgo alto: un fallo en el cortafuegos compromete toda la red interna.
* **Arquitectura fuerte**:
  + DMZ protegida por dos cortafuegos:
    - Cortafuegos externo: bloquea tráfico no deseado desde la red externa hacia la DMZ.
    - Cortafuegos interno: evita que tráfico no autorizado pase de la DMZ a la red interna.
  + Ventaja: Si uno falla, el daño se limita a una parte de la red.

**Página 10-11: Host Bastión**

* **Definición**:
  + Equipo o servidor diseñado para resistir ataques y ofrecer un único servicio (correo, web, proxy, etc.).
* **Características**:
  + Altamente expuesto a ataques; fortificación sólida para minimizar riesgos.
  + Protocolos y servicios innecesarios deshabilitados.
  + Puede usarse como señuelo (honeypot) para analizar intentos de intrusión.

**Página 12-16: Cortafuegos (Firewalls)**

* **Funciones**:
  + Controlan el tráfico entre redes, asegurando que solo pasen datos autorizados.
* **Modos de operación**:
  + **Filtrado estático**: Basado en reglas fijas que consideran IPs, puertos y protocolos.
    - Ejemplo: Listas blancas (política restrictiva) o negras (política permisiva).
  + **Filtrado dinámico**: Reglas creadas y destruidas según conexiones activas.
    - Solo se permite el tráfico externo que responda a una conexión interna previa.
* **Limitaciones**:
  + Vulnerabilidad a suplantación de IPs.
  + Problemas con servicios que usan puertos no estándar.

**Página 17-18: Redes Privadas Virtuales (VPN)**

* **Definición y funcionamiento**:
  + Conexión cifrada entre dos puntos a través de Internet, conocida como "túnel VPN".
* **Usos**:
  + Interconexión de filiales, empleados remotos y clientes de manera segura.
* **Ventajas**:
  + Menores costos comparados con líneas dedicadas.
  + Incrementa confidencialidad y seguridad de datos.
* **Desventajas**:
  + Requiere recursos computacionales para el cifrado.
  + Dependencia de Internet como red subyacente.

**Página 19-22: Zona Desmilitarizada (DMZ)**

* **Definición**:
  + Red intermedia que separa los equipos públicos (expuestos al exterior) de la red interna.
* **Importancia**:
  + Permite controlar conexiones hacia servidores públicos mientras protege datos internos.
* **Elementos clave**:
  + Diseño flexible para adaptarse a necesidades de seguridad.
  + Uso de cortafuegos para segmentar tráfico según protocolos y puertos.

**Página 23-25: IDS (Sistema de Detección de Intrusos)**

* **Características**:
  + Opera continuamente sin intervención humana.
  + Detecta desviaciones en el comportamiento estándar del sistema.
* **Fortalezas**:
  + Detección de ataques en tiempo real.
  + Ayuda a rastrear la fuente de los ataques.
* **Limitaciones**:
  + Genera falsas alarmas.
  + Requiere ajuste constante para adaptarse a cambios en el comportamiento de la red.

**Página 26-27: Filtrado de Paquetes Estático**

* **Definición**:
  + Método básico de los cortafuegos para aceptar o rechazar paquetes según parámetros específicos, como:
    - Dirección IP de origen/destino.
    - Número de puerto.
    - Campos en la cabecera (por ejemplo, flags TCP como SYN o ACK).
* **Modos de configuración**:
  + **Política restrictiva (Lista blanca)**:
    - Bloquea todo el tráfico por defecto, permitiendo únicamente lo especificado explícitamente.
  + **Política permisiva (Lista negra)**:
    - Permite todo el tráfico por defecto, bloqueando solo lo que se especifique.
* **Problemas del filtrado estático**:
  + Las direcciones IP pueden ser falsificadas.
  + Puertos no estándar dificultan la identificación de servicios.
  + No soporta comportamientos dinámicos ni autenticación robusta.

**Página 28: Filtrado de Paquetes Dinámico**

* **Definición**:
  + Reglas de filtrado que se crean y destruyen dinámicamente en función de las conexiones activas.
* **Funcionamiento**:
  + Los paquetes de salida permitidos generan automáticamente reglas para aceptar las respuestas correspondientes.
  + Solo se permite la entrada de paquetes que sean respuestas a solicitudes realizadas desde la red interna.
* **Ventajas**:
  + Adaptabilidad a conexiones legítimas, asegurando que las respuestas lleguen.
* **Desventajas**:
  + Limitado al análisis de cabeceras de paquetes; no puede filtrar por otros parámetros.

**Páginas 29-32: Redes Privadas Virtuales (VPN)**

* **Funcionamiento**:
  + Se basa en el uso de un protocolo de túnel que cifra los datos desde el origen hasta el destino.
  + Componentes:
    - **Cliente VPN**: Cifra/descifra datos desde el lado del usuario.
    - **Servidor VPN**: Descifra los datos en la red corporativa y los envía de vuelta cifrados.
* **Usos**:
  + Interconexión segura entre filiales.
  + Acceso remoto para empleados.
* **Ventajas**:
  + Reducción de costos al usar infraestructura pública.
  + Seguridad mejorada con cifrado y autenticación.
* **Desventajas**:
  + Consumo de recursos computacionales para cifrado.
  + Necesidad de supervisión constante por parte del administrador.

**Páginas 33-34: ¿Qué es una Red DMZ?**

* **Definición**:
  + Segmento intermedio entre la red interna y externa que permite un nivel adicional de seguridad.
* **Propósito**:
  + Permitir conexiones controladas a servidores públicos (web, correo, DNS), mientras se protege la red interna.
* **Diseño Básico**:
  + Las conexiones de la red interna y externa solo pueden alcanzar la DMZ.
  + Los dispositivos en la DMZ no tienen acceso directo a la red interna.
* **Importancia del diseño**:
  + La ubicación de los servidores y el tipo de servicios ofrecidos determinan la efectividad de la DMZ.
  + Se deben considerar las vulnerabilidades de los protocolos utilizados.

**Páginas 35-37: Características y Usos del IDS**

* **Características del IDS**:
  + Funciona en segundo plano sin necesidad de supervisión constante.
  + Detecta desviaciones en el comportamiento estándar de la red.
  + Soporta fallos, monitorizando incluso en situaciones adversas.
* **Fortalezas**:
  + Proporciona información sobre intentos de intrusión.
  + Actúa como elemento disuasorio y permite reaccionar ante ataques.
  + Menor costo de implementación al ubicarse en puntos estratégicos.
* **Limitaciones**:
  + Alta tasa de falsas alarmas.
  + Requiere actualización y adaptación constante para ser efectivo.
  + No sustituye otras herramientas como cortafuegos o auditorías de seguridad.

**Página 38: Resumen Final**

* **Elementos esenciales de la seguridad perimetral**:
  + Uso de cortafuegos para controlar tráfico entre redes.
  + Implementación de DMZ para exponer servicios públicos sin comprometer la red interna.
  + Adopción de VPN para conexiones remotas seguras.
  + Monitorización constante con IDS para detectar ataques y anomalías.
* **Importancia de la defensa en profundidad**:
  + Cada capa adicional de seguridad reduce el riesgo y minimiza el impacto de posibles fallos.