Análisis de Arquitectura de Red para la Implementación de IDS/IPS

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@June 25, 2024
Wochentage	Dienstag
Deadline	@June 25, 2024
Status	Sended

Instrucciones

En esta tarea, vamos a analizar una arquitectura de red y determinar los puntos óptimos para la instalación de Sistemas de Detección de Intrusos (IDS) y Sistemas de Prevención de Intrusos (IPS). Su objetivo es identificar y justificar los lugares adecuados para la implementación de IDS/IPS, así como decidir el tipo de sistema que debe ser utilizado (NIDS, HIDS o un enfoque híbrido).

Pasos a seguir:

1. **Revisión de la Arquitectura de Red**
    - Examine la arquitectura de red proporcionada en los recursos de la clase. Preste atención a los diferentes segmentos de la red, como la DMZ, la red interna, los servidores y los puntos de acceso a internet.
2. **Identificación de Puntos Críticos**
    - Identifique los puntos críticos dentro de la arquitectura de red donde la implementación de IDS/IPS sería más beneficiosa. Estos puntos pueden incluir puertas de enlace, servidores críticos, segmentos de red internos y perimetrales.
3. **Selección del Tipo de IDS/IPS**
    - Decida si un Sistema de Detección de Intrusos (IDS) o un Sistema de Prevención de Intrusos (IPS) sería más adecuado para cada punto crítico identificado. Justifique su decisión.
    - Determine el tipo de sistema que debe ser implementado:
        - **NIDS (Network-based IDS)**: Para monitorear el tráfico de red en tiempo real.
        - **HIDS (Host-based IDS)**: Para monitorear la actividad en un host específico.
        - **Híbrido**: Una combinación de NIDS y HIDS para una cobertura más completa.
4. **Justificación de la Implementación**
    - Explique por qué ha seleccionado cada punto para la implementación de IDS/IPS.
    - Proporcione una breve justificación para la elección del tipo de IDS/IPS en cada caso.
5. **Diagrama Anotado**

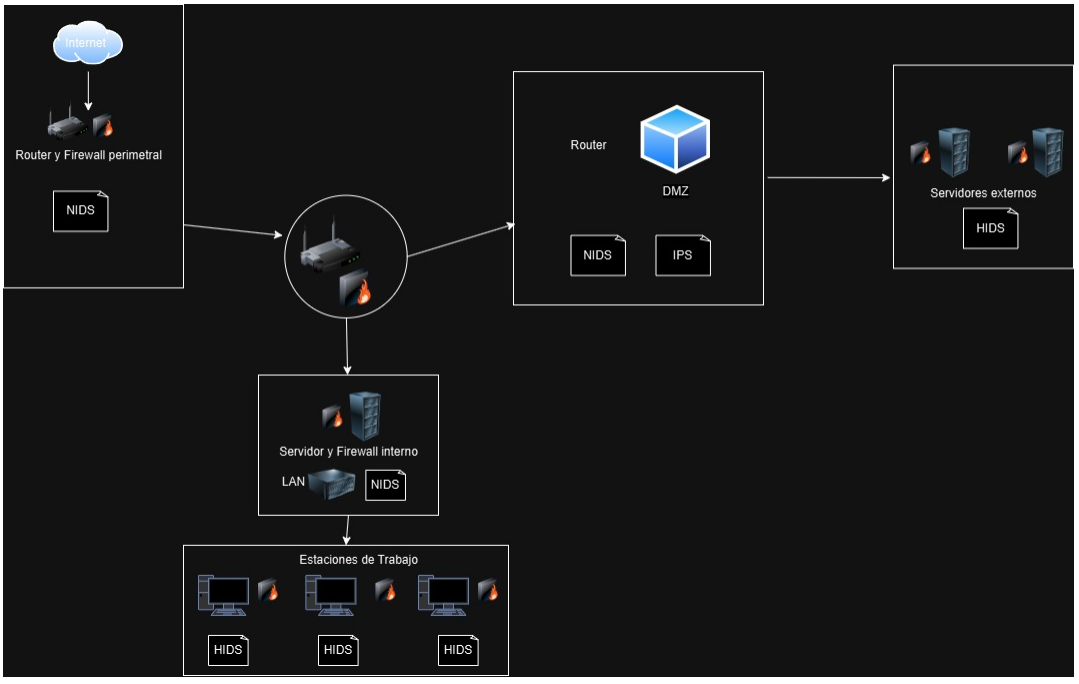
- Utilice una herramienta de diagramación (como draw.io, Microsoft Visio, Lucidchart, o una herramienta de diagramación en línea) para crear un diagrama de la arquitectura de red con anotaciones que muestren dónde se instalarán los IDS/IPS y de qué tipo.

Entregables:

- **Presentación en clase**
- **Diagrama de Red Anotado**
  - Un diagrama de la arquitectura de red con las ubicaciones y tipos de IDS/IPS claramente marcados y anotados y justificados.

Desarrollo

Gráfico



Revisión de la arquitectura de red

La arquitectura de red está diseñada para maximizar la seguridad mediante la segmentación y el uso de dispositivos de seguridad en múltiples capas. La red se organiza en los siguientes segmentos:

1. **Internet**

2. **Router y Firewall Perimetral con NIDS**
3. **Router Principal con Firewall**
4. **DMZ con NIDS e IPS**
5. **Servidores Externos con Firewalls y HIDS**
6. **Servidor y Firewall Interno**
7. **LAN con NIDS**
8. **Estaciones de Trabajo con Firewalls y HIDS**

Identificación de puntos críticos

- **Internet y Perímetro de la Red**:
  - **Dispositivos**: Router y Firewall Perimetral, NIDS.
  - **Justificación**: La primera línea de defensa contra ataques externos. El NIDS monitoriza el tráfico entrante y saliente para detectar posibles amenazas antes de que ingresen a la red.
- **DMZ**:
  - **Dispositivos**: NIDS, IPS.
  - **Justificación**: La DMZ aloja servidores accesibles desde Internet, como servidores web y de correo. El NIDS monitoriza el tráfico en la DMZ, y el IPS bloquea activamente cualquier intento de intrusión detectado.
- **Servidores Externos en la DMZ**:
  - **Dispositivos**: Firewalls, HIDS.
  - **Justificación**: Los servidores críticos necesitan protección adicional. Los HIDS monitorizan actividades específicas en cada servidor para detectar accesos no autorizados y otras actividades sospechosas.
- **Red Interna (LAN)**:
  - **Dispositivos**: NIDS.
  - **Justificación**: La LAN interna necesita monitoreo para detectar actividades sospechosas que podrían moverse lateralmente dentro de la red.
- **Estaciones de Trabajo**:

- **Dispositivos**: Firewalls, HIDS.
- **Justificación**: Cada estación de trabajo está protegida por un firewall y un HIDS para monitorear y bloquear accesos no autorizados y actividades anómalas a nivel del host.

Selección del Tipo de ISD/IPS

- **NIDS (Network-based IDS)**:
  - **Ubicación**: Perímetro de la red, DMZ, LAN.
  - **Función**: Monitorear el tráfico de red en tiempo real para detectar actividades sospechosas y posibles intrusiones.
  - **Justificación**: Proporciona una visión general del tráfico de red, permitiendo la detección de patrones de ataque y anomalías.
- **HIDS (Host-based IDS)**:
  - **Ubicación**: Servidores Externos, Estaciones de Trabajo.
  - **Función**: Monitorear la actividad en un host específico, como cambios en archivos, intentos de acceso, y actividades de usuarios.
  - **Justificación**: Proporciona una capa de seguridad granular a nivel del host, detectando amenazas que podrían no ser visibles a nivel de red.
- **IPS (Intrusion Prevention System)**:
  - **Ubicación**: DMZ.
  - **Función**: Bloquear activamente intentos de intrusión en tiempo real.
  - **Justificación**: Previene ataques antes de que puedan afectar a los servidores críticos en la DMZ.

Justificación de la Implementación

- **Internet y Perímetro de la Red**:
  - **NIDS**: Colocado aquí para detectar ataques y tráfico sospechoso antes de que lleguen a los componentes internos de la red. Esto es crítico para identificar amenazas externas desde el principio.
- **DMZ**:

    - **NIDS**: Monitoriza todo el tráfico dentro de la DMZ, proporcionando visibilidad sobre posibles ataques a los servidores en esta zona.
    - **IPS**: Implementado para detener ataques en tiempo real, protegiendo los servidores críticos de accesos no autorizados y ataques DDoS.
- **Servidores Externos en la DMZ**:
    - **HIDS**: Proporcionan monitoreo específico en cada servidor, detectando cambios no autorizados, accesos y comportamientos anómalos que podrían indicar una intrusión.
- **Red Interna (LAN)**:
    - **NIDS**: Monitoriza el tráfico interno, detectando posibles amenazas que han atravesado otras capas de seguridad o que se originan dentro de la red interna.
- **Estaciones de Trabajo**:
    - **HIDS**: Proporcionan una capa adicional de seguridad en cada estación de trabajo, detectando y respondiendo a actividades sospechosas y accesos no autorizados a nivel del host.
    - **Firewalls**: Cada estación de trabajo está protegida por un firewall para controlar el tráfico entrante y saliente, previniendo accesos no autorizados.
