Documento de Alcance

TI - Sistemas IPS e IPD

Seguridad en Redes

Docente: Ing. Gonzalo Vilanova

Alumna: Flavia De Rosa

Legajo: 158.739-0

Comisión: K4571

Breve introducción:

Los IDS/IPS son un complemento que ofrece mayor seguridad a las redes de distintos tamaños, principalmente aquellas redes que requieren un alto nivel de respuesta y servicios. Estos sistemas pueden aplicarse a software o hardware. Tienen la capacidad de detectar ataques cibernéticos y realizar las acciones necesarias para anular los efectos dañinos que se pudieran ocasionar a la red.

Alcance - Temas a desarrollar

1. ¿Qué es IDS (Intrusion Detection System)?
    a. Componentes
    b. Funcionamiento - Detección de Anomalías
    c. Tipos de IDS
        i. NIDS (NetworkIDS)
        ii. HIDS (HostIDS)
    d. IDS más conocidos
        i. Snort
        ii. Ossec
    e. Importancia

2. ¿Qué es IPS (Intrusion Preventions System)?
    a. Funcionamiento Arquitectura
    b. Análisis de respuestas
    c. Tipos de IPS

3. ¿Qué es SIEM (Security Information and Event Management)?
    a. Tipos de SIEM
    b. Herramientas que utiliza
    c. Comparativa con IDS/IPS

4. Herramientas que incluyen paquete de IDS e IPS
    a. Security Onion
    b. WinPatrol

5. Sistemas IDS/IPS vs Firewall
    a. Ventajas
    b. Desventajas

6. Sistemas IDS/IPS vs UTM(Unified Threat Management)
    a. Ventajas
    b. Desventajas