Guia Seguridad

Sistemas Distribuidos 2C 2025

1. ¿Qué protocolos o herramientas de seguridad se pueden utilizar para superar los siguientes desafíos?
    a. Garantizar la integridad del mensaje.
    b. Autenticación mutua.
    c. Suplantación de identidad.
    d. Ataques de replicación.
    e. Gestionar eficientemente las claves secretas compartidas en sistemas grandes.
    f. Autenticidad de las claves públicas.
    g. No revelar información sensible antes de la autenticación de las partes.
2. ¿Por qué se usan claves de sesión? ¿Qué beneficios tiene?
3. Identifique la política de acceso que aplica a cada escenario:
    a. Un alumno crea un nuevo archivo con el informe de Física III. Por defecto, solo él puede leer y modificar el archivo. Decide otorgar permisos de lectura y escritura a todo su equipo y, además, da permiso de comentar a los profesores.
    b. En un hospital, el acceso a los sistemas de información está estrictamente organizado. Un usuario con el perfil de "Médico" puede acceder a los historiales clínicos de los pacientes que tiene asignados, solicitar pruebas y ver sus resultados. Un usuario con el perfil de "Administrativo" puede acceder a la información de facturación de los pacientes y gestionar las citas, pero no puede ver los detalles clínicos del historial. Por último, un usuario con el perfil de "Director de Hospital" puede ver reportes estadísticos y de gestión, pero no tiene acceso a los historiales individuales de los pacientes.
    c. En una agencia de seguridad nacional, todos los documentos y usuarios están clasificados con etiquetas de seguridad como "Público", "Confidencial", "Secreto" y "Top Secret". Un usuario con autorización "Secreto" puede acceder libremente a documentos clasificados como "Público" y "Confidencial", pero el sistema le denegará automáticamente el acceso a cualquier documento etiquetado como "Top Secret". Estas reglas son configuradas por un administrador central de seguridad y no pueden ser modificadas por los usuarios.
    d. Una aplicación bancaria moderna implementa políticas de seguridad muy dinámicas. Por ejemplo, un cliente puede realizar transferencias de hasta 1.000 € desde su propia red Wi-Fi registrada y durante el horario diurno (9:00 a 20:00). Sin embargo, si el mismo cliente intenta realizar una transferencia de más de 500 € mientras está conectado a una red Wi-Fi pública en otro país, el sistema bloquea la operación y solicita una segunda forma de autenticación (ej. una llamada de confirmación). La política evalúa el rol del usuario (cliente), la ubicación, la seguridad de la red, la cantidad de la transacción y la hora del día antes de permitir o denegar la operación.

4. ¿Cuál es la principal diferencia entre un firewall de filtrado de paquetes y un gateway a nivel de aplicación? De un ejemplo de ambos.
5. Busque ejemplos reales de mecanismos de Detection Intrusion Para *signature-based Intrusion Detection Systems* y *Anomaly-based Intrusion Detection Systems*