Informe Técnico de Diagnóstico: Análisis de Falla de Red usando Modelos OSI y TCP/IP

Auditor: Especialista en Seguridad Ofensiva / Ethical Hacking
Entidad Auditada: [Nombre de la Empresa]
Clasificación: Interno – Diagnóstico de Infraestructura
Fecha: [Fecha del análisis]

Introducción

En el contexto de una auditoría de seguridad y operación de redes internas, se simuló un escenario en el cual empleados de la organización no podían acceder al sitio web corporativo interno (`http://intranet.empresa.local`), pese a que la conexión a Internet externa funcionaba con normalidad. Este tipo de fallo es común en entornos empresariales con servicios segmentados y sistemas internos autogestionados.

El presente informe aplica los modelos OSI y TCP/IP como marcos metodológicos para identificar, interpretar y diagnosticar la causa raíz de esta falla, con un enfoque profesional y sistemático basado en capas.

Escenario Evaluado

- Acceso a Internet confirmado (Google, correo web, etc.)
- Inaccesibilidad específica a la dirección `http://intranet.empresa.local`
- Infraestructura mixta con resolución DNS interna
- Usuarios afectados en distintas áreas de la red

Este patrón sugiere un **problema localizado en el entorno interno** de red, sin indicios de caídas en la conectividad general o del proveedor externo.

Diagnóstico por Modelo OSI (Capas 1 a 7)

Capa Física
Se verificó la presencia de conectividad física adecuada: cables conectados, luces activas en switches, interfaces habilitadas en los dispositivos cliente. No se identificaron problemas de hardware o desconexión.

Capa de Enlace de Datos
La interfaz de red estaba activa, sin errores de transmisión en los logs del sistema operativo. No se detectaron colisiones ni pérdida de tramas. La MAC estaba correctamente asociada a la VLAN interna.

Capa de Red
Los equipos tenían IP válidas dentro del rango corporativo. Sin embargo, al ejecutar `ping intranet.empresa.local`, no se obtuvo respuesta. El `ping` a la IP directa del servidor respondió exitosamente, lo que descarta pérdida de conectividad y apunta a un fallo en la resolución de nombres.

Capa de Transporte
Se ejecutó `telnet intranet.empresa.local 80`, lo que no generó conexión. Posteriormente se probó `telnet [IP directa] 80` con éxito, indicando que el puerto está abierto y activo, pero el dominio no se resuelve correctamente.

Capa de Sesión y Presentación
No se detectaron errores de sesión HTTP al usar IP directa. No se observaron fallos en la codificación ni incompatibilidades en la representación de los datos.

Capa de Aplicación
El servidor web se encontraba corriendo (Apache 2.4). El sitio responde por IP, pero no por dominio local. Esto indica que la falla se ubica en la capa de aplicación relacionada con el servicio de resolución de nombres, probablemente el DNS interno.

Diagnóstico por Modelo TCP/IP

Capa de Acceso a Red
Verificación positiva de cableado, conectividad LAN y asociación DHCP/estática. La red no presentaba interferencias ni segmentaciones anómalas.

Capa de Internet
La herramienta `nslookup intranet.empresa.local` no devolvió una IP válida. Esto confirma la hipótesis de fallo en el servicio DNS interno o en la configuración del archivo de zonas del dominio local.

Capa de Transporte
El puerto 80 del servidor responde correctamente al usar la IP. El firewall interno permite la conexión HTTP sin filtrado explícito en ese segmento.

Capa de Aplicación
El servidor HTTP está activo, responde a peticiones y entrega contenido esperado cuando se accede por IP. La falla no se encuentra en la lógica de la aplicación, sino en el mecanismo de acceso (resolución de nombre).

Blandskron

Hipótesis Técnica de la Falla

> El servicio DNS interno no está resolviendo correctamente el dominio `intranet.empresa.local`, impidiendo que las estaciones cliente accedan al recurso usando su nombre. Dado que el acceso por IP directa sí funciona, se descarta una caída del servicio HTTP, del sistema operativo del servidor, o del enlace físico.

Pruebas Realizadas para Validación

- **`ping intranet.empresa.local`** → No responde
- **`ping [IP del servidor]`** → Responde correctamente
- **`nslookup intranet.empresa.local`** → Falla en resolución (no devuelve IP)
- **`telnet intranet.empresa.local 80`** → Falla
- **`telnet [IP directa] 80`** → Conexión establecida
- **Acceso web por IP** → El contenido del sitio se muestra correctamente

Conclusión Profesional

La causa raíz del fallo es una disfunción en la resolución DNS interna, que impide que los clientes puedan convertir el nombre `intranet.empresa.local` en una dirección IP válida. No existe bloqueo a nivel de firewall, ni falla de red, ni error en el servicio HTTP.

El entorno operativo del servidor está funcional, y las capas inferiores del modelo OSI están estables.

Recomendaciones Técnicas

1. **Revisar el servidor DNS interno**
   Validar el archivo de zonas, los registros A, y el servicio en ejecución. Reiniciar `bind`, `dnsmasq`, o el controlador DNS en Windows Server si corresponde.

2. **Actualizar registros en hosts (temporal)**
   Como medida de contingencia, añadir manualmente el dominio e IP en el archivo `hosts` de los clientes para permitir acceso mientras se corrige el DNS.

3. **Verificar políticas de red interna**
   Asegurarse de que las solicitudes DNS no estén siendo redirigidas a servidores

externos sin autoridad sobre el dominio local.

4. **Implementar pruebas programadas**
   Automatizar chequeos de resolución DNS y disponibilidad de puertos críticos para anticipar futuras fallas.

5. **Actualizar documentación interna**
   Confirmar que el dominio `empresa.local` esté registrado correctamente y que la política de nombres no entre en conflicto con otros dominios de prueba o servicios cloud (como Microsoft 365).