Informe Técnico: Análisis de Comunicación HTTP Basado en Modelos OSI y TCP/IP

Autor: Equipo de Seguridad Ofensiva
Entidad Auditada: [Nombre de la Empresa]
Fecha: [Fecha del informe]
Clasificación: Uso Interno – Revisión de Red

Introducción

Durante el proceso de auditoría ética de red, se ejecutó un ejercicio simulado de acceso a recursos web externos con el fin de evidenciar las capas, protocolos y funciones involucradas en una transacción cliente-servidor típica. Este análisis busca demostrar la interacción entre los modelos OSI y TCP/IP en una solicitud HTTP estándar, ayudando a identificar potenciales puntos de falla, interceptación o malconfiguración.

Contexto de Análisis

El escenario emulado consistió en una acción cotidiana: un usuario accede al sitio web `www.ejemplo.com` desde una estación cliente conectada a la red corporativa. Este evento desencadena una secuencia de interacciones protocolarias entre capas lógicas, que en conjunto forman la base técnica para la entrega de servicios web.

El análisis se enfocó en la correcta identificación de las capas involucradas, los protocolos utilizados y los vectores técnicos que un atacante podría comprometer si no se aplican controles adecuados.

Flujo de Comunicación y Capas Involucradas

Ingreso de la URL
El usuario introduce la dirección web en su navegador. Este evento corresponde a la **capa de aplicación** (modelo OSI) y utiliza el protocolo **HTTP**. Aquí se inicia la generación de una solicitud HTTP formal.

Establecimiento de conexión
El navegador establece una conexión TCP con el servidor remoto en el puerto 80. Esta acción ocurre en la **capa de transporte**, utilizando el protocolo **TCP**, que garantiza una comunicación confiable mediante el mecanismo de triple handshake.

Resolución de dominio y direccionamiento
El sistema cliente consulta un servidor DNS para obtener la dirección IP correspondiente a `www.ejemplo.com`. Este proceso ocurre en la **capa de red**, donde se aplica el protocolo **IP**, y donde el servicio de resolución de nombres (DNS) actúa indirectamente.

Transmisión física y lógica de datos
Los paquetes se encapsulan dentro de tramas Ethernet (o Wi-Fi, según el medio), y se transmiten a través de interfaces de red. Este paso involucra la **capa de enlace de datos** y la **capa física**, responsables del direccionamiento MAC y la conversión de datos a señales eléctricas u ópticas.

Recepción y respuesta del servidor
El servidor web recibe la solicitud, procesa la ruta solicitada y responde mediante el mismo canal. El contenido recorre las capas en orden inverso desde el servidor hacia el cliente.

Correspondencia de Protocolos y Capas OSI

- **HTTP** → Capa de Aplicación
  Proporciona el mecanismo de solicitud/respuesta para acceso a recursos web.

- **TCP** → Capa de Transporte
  Asegura la entrega ordenada y libre de errores.

- **IP** → Capa de Red
  Provee direccionamiento lógico y enrutamiento interred.

- **Ethernet / Wi-Fi (IEEE 802.11)** → Capa de Enlace de Datos
  Controla el acceso al medio y la entrega local punto a punto.

Funciones Clave por Capa Analizadas

Capa Física
Encargada de la transmisión binaria sobre el medio físico. Cualquier interrupción o interferencia en esta capa puede derivar en pérdida total de conectividad.

Capa de Red
Determina la ruta y asegura el encaminamiento de paquetes a través de múltiples dispositivos intermedios. Errores aquí pueden causar fallos de resolución o pérdida de paquetes.

Capa de Transporte
Gestiona la integridad de los datos y el control de flujo. Ataques de denegación de servicio o escaneos de puertos suelen dirigirse contra esta capa.

Capa de Aplicación
Responsable de entregar servicios directamente al usuario. Es un vector común de ataques como inyección, manipulación de cabeceras, y explotación de servidores mal configurados.

Esquema General del Flujo de Datos

[Navegador cliente]

↓

[Capa de Aplicación - HTTP]

↓

[Capa de Transporte - TCP]

↓

[Capa de Red - IP]

↓

[Capa de Enlace - Ethernet/Wi-Fi]

↓

[Internet / ISP / Enrutadores]

↓

[Servidor Web - www.ejemplo.com]

↑

[Respuesta vía las mismas capas]

Observaciones del Equipo de Auditoría

- La estructura por capas facilita una comprensión ordenada de la comunicación, pero también señala con claridad posibles puntos de intervención maliciosa.

- En redes reales, cada una de estas capas debe ser protegida con controles específicos (ej. cifrado TLS en capa 7, filtrado de paquetes en capa 3, aislamiento

físico y monitoreo en capa 1).

- Las solicitudes HTTP sin cifrar (puerto 80) son altamente susceptibles a inspección y manipulación. Se recomienda deshabilitar HTTP no seguro o redireccionarlo automáticamente a HTTPS.

- La resolución DNS puede ser interceptada o manipulada mediante ataques como spoofing si no se utilizan mecanismos como DNSSEC o DoH (DNS over HTTPS).

Recomendaciones Técnicas

1. **Aplicar inspección TLS** en gateways corporativos para mitigar tráfico inseguro.

2. **Restringir puertos** innecesarios a nivel de firewall interno y de borde.

3. **Usar herramientas de monitoreo** para auditar el comportamiento real de las solicitudes (ej. Wireshark, Zeek, ELK stack).

4. **Entrenar al personal técnico** en lectura y diagnóstico de tráfico HTTP, trazas TCP y resolución DNS.

5. **Implementar políticas de hardening** sobre navegadores, configuraciones de red y servidores internos.

Conclusión

El análisis de la comunicación HTTP desde una perspectiva de capas demuestra que cada interacción digital involucra múltiples niveles de procesamiento técnico, cada uno con potenciales puntos de fallo o explotación. Una arquitectura segura no depende solo del firewall, sino del entendimiento profundo de cómo fluye la información. La identificación de protocolos, rutas y funciones es la base para una red robusta y resiliente frente a amenazas.