

SMB (SERVER MESSAGE BLOCK)

Administración de sistemas y redes 5AO 2025

Federico Greco, Ignacio Comin, Rocío Penalva

¿Qué es SMB?

Protocolo de red de nivel de aplicación.

Permite compartir archivos, impresoras y otros recursos

Opera en modo cliente-servidor

Usado en redes locales (hogar y empresas)



Funcionamiento

Modelo cliente-servidor

Opera sobre TCP/IP (puerto 445) o NetBIOS (p 137-139)

Utiliza comandos para gestionar archivos y sesiones

Autenticación de usuarios y control de acceso



Historia

Creado por IBM en 1983

Adoptado por Microsoft en sistemas Windows

Evolución desde SMB 1.0 hasta SMB 3.0

Mejora en seguridad, rendimiento y compatibilidad





HISTORIA

SMB 1.0 (CIFS)

Versión original

Usado en redes Windows antiguas

Comunicación sobre NetBIOS

+100 comandos (archivos, impresoras, mailslots)

Seguridad débil → obsoleto y vulnerable



SMB 2.0 (Vista/Server 2008)

Menos comandos, mayor escalabilidad, mejor rendimiento en redes modernas

Encabezado fijo (64 bytes)

TCP 445 directo (sin NetBIOS)

Compounding: varias operaciones en un solo paquete

Durable handles: reconexión tras cortés

Firma con **HMAC-SHA256**



SMB 2.1 (Windows 7/Server 2008 R2)

Mejoras de rendimiento

Soporte avanzado para **BranchCache** (oficinas remotas)

Optimización de **MTU** (ajuste de tamaños para red)

Más estabilidad en entornos distribuidos

Mecanismos de bloqueo



SMB 3.0 (Windows 8/Server 2012)

Alto rendimiento y resiliencia

SMB Multichannel: múltiples rutas de red → +ancho de banda y tolerancia a fallos

SMB Direct (RDMA): baja latencia y menor uso de CPU

Failover transparente: reconexión automática en clústeres

Directory leasing: reduce latencia en directorios



SMB 3.0 (Seguridad)

Cifrado nativo y protección avanzada

Cifrado de extremo a extremo (AES-CCM) sin usar IPSec

Negociación segura de dialectos: detecta ataques downgrade

Firmas mejoradas y contadores de rendimiento

Integración con PowerShell para gestión avanzada




SMB 3.02 y 3.1.1

SMB 3.02 (Windows 8.1)

- Optimiza balanceo de carga
- Optimización de copia remota (archivos WAN)
- Mejorar operaciones I/O

SMB 3.1.1 (Windows 10)

- Integridad previa a la autenticación (contra ataques MitM)
 - Nuevas suites de cifrado y firma
 - Máxima seguridad del protocolo hasta hoy
- 



¿CÓMO FUNCIONA?

Comunicación Cliente-Servidor

SMB permite que un cliente acceda a recursos compartidos en otros dispositivos de la red.

- Cliente y servidor deben tener implementaciones compatibles.
- El cliente envía solicitudes; el servidor las procesa con un servicio SMB activo.

Antes de transferir datos:

- Se establece una conexión lógica.
- Se negocia la versión de SMB y se realiza la autenticación.



Conexión y transmisión

SMB viaja sobre **TCP/IP**, puerto **445**.

Se establece conexión con **three-way handshake** (SYN → SYN-ACK → ACK).

Una vez conectados:

- SMB gestiona el intercambio de mensajes estructurados.
- Se asegura **fiabilidad, control de flujo y corrección de errores** gracias a TCP.





¿DÓNDE SE IMPLEMENTA?

Implementaciones más conocidas

Samba: implementación libre de SMB para Linux/Unix. Permite interoperabilidad con sistemas Windows.

ConnectedNAS: app para Android que actúa como cliente y servidor SMB (desde la versión 2 por seguridad).

Hyper-V + SMB 3.0: permite guardar archivos de máquinas virtuales (VHD, config, snapshots) en recursos compartidos.

SQL Server + SMB: soporta guardar bases de datos en recursos SMB. Desde SQL Server 2008 R2 y versiones posteriores.




PROBLEMAS DE SEGURIDAD

Vulnerabilidades

EternalBlue: Falla en SMBv1 filtrada por *Shadow Brokers* en 2017. Permite ejecución remota de código sin intervención del usuario.

EternalRomance: También por *Shadow Brokers*. Afecta sistemas sin parches y permite control remoto total con paquetes maliciosos.

SMBGhost y SMBleed: Vulnerabilidades en SMBv3. Permiten ejecución remota de código y exfiltración de memoria del núcleo, comprometiendo el sistema.



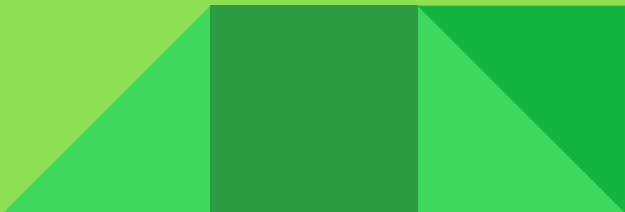
Incidentes

WannaCry (2017): Usó la vulnerabilidad EternalBlue en SMBv1 para cifrar archivos y pedir rescate en bitcoin; afectó 200,000 equipos en 150 países.

Petya (2016): Inicialmente por phishing, luego usó EternalBlue para cifrar archivos y propagarse lateralmente en redes.

NotPetya (2017): Diseñado para destruir datos, cifrando y dañando archivos sin intención de solicitar nada para el rescate.

SMB es objetivo de ataques que permiten acceso no autorizado, movimiento lateral y robo de datos en redes.



Ataques

Fuerza bruta: Múltiples combinaciones de usuarios y contraseñas para acceder y robar o modificar datos.

Ataques Man-in-the-Middle (MitM): Interceptan y manipulan la comunicación cliente-servidor, robando credenciales o datos.

Ataques DDoS: Saturan el servicio SMB con solicitudes falsas, causando interrupciones y posibles distracciones para otros ataques.





¿ES SEGURO?


Recomendado a partir de SMB 3.0 (3.1.1)

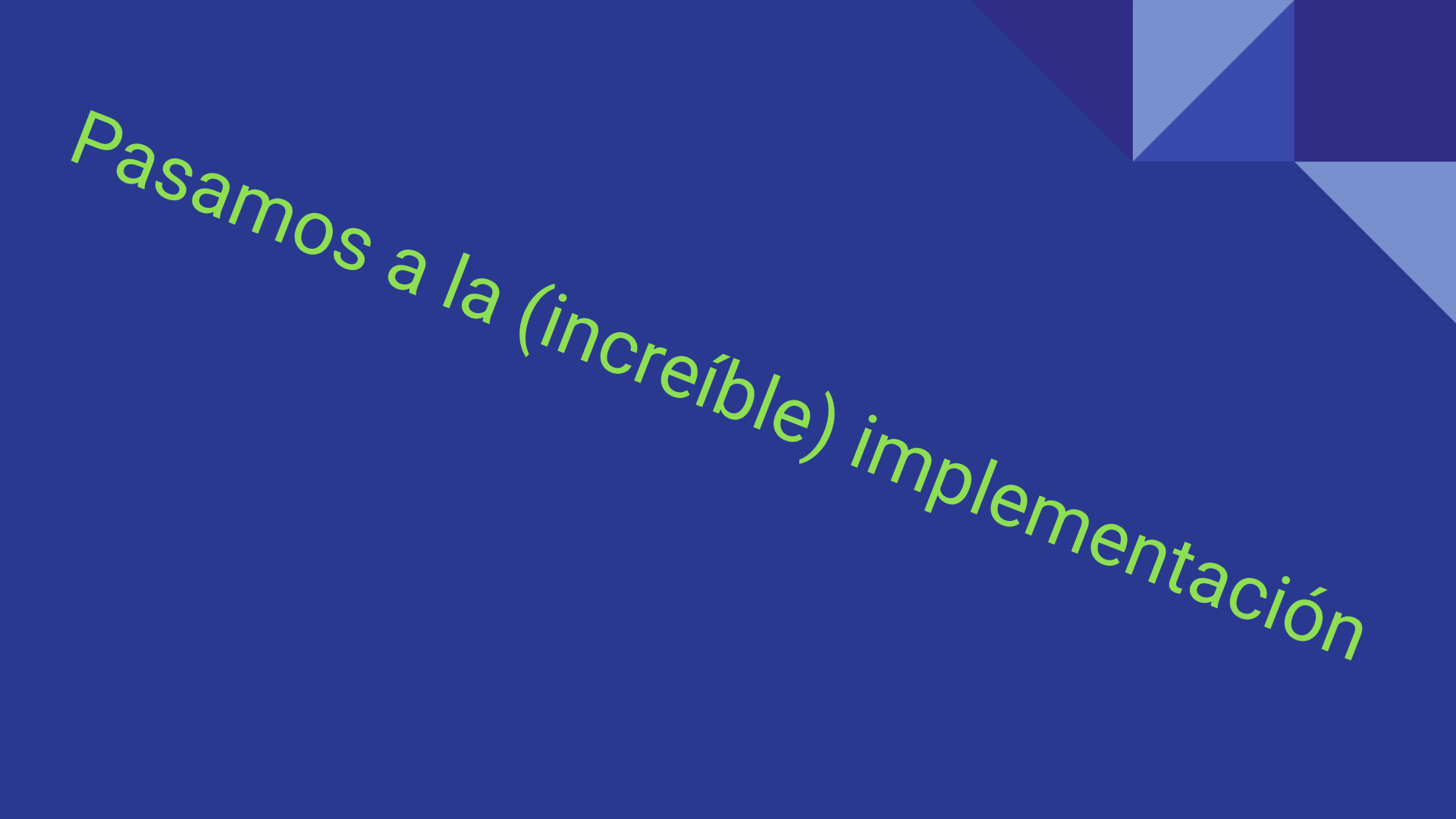
SMB 1.0: Sin cifrado nativo. Se usaba **IPSec** para confidencialidad. Muy vulnerable y **debe desactivarse** si no es estrictamente necesario.

SMB 2.x: Mejora la seguridad, aún **sin cifrado**, pero con **firma obligatoria** en entornos de dominio.

SMB 3.0 / 3.02: Introduce **SMB Encryption** con **AES**. Cifrado por recurso o global. Mejora la integridad.

SMB 3.1.1: Agrega **Preauthentication Integrity** (protege desde el inicio de sesión). Recomendado por Microsoft para enlaces críticos.





Pasamos a la (increíble) implementación



MUCHAS GRACIAS