El protocolo ACME (Automated Certificate Management)

Permite que un servidor web, a través de un cliente ACME (como Certbot), pueda comunicarse directamente con una CA como letsEncrypt) para solicitar, validar y obtener un certificado, todo sin intervención humana

La parte más crítica del protocolo ACME es la validación del dominio para evitar suplantaciones de identidad

Desafío HTTP-01: la CA te pide que sirvas un archivo específico como un nombre y contenido exactos en una URL determinada de tu dominio.

Desafío DNS-01: la CA te pide crear un registro de tipo TXT con un nombre y un valor específico

SSL 2.0 y SSL 3.0

El Problema: Ambos protocolos tienen fallas de diseño graves e irreversibles. La vulnerabilidad mas famosa es el ataque POODLE (Padding Oracle On Downgraded Legacy Encryption) en SSL3.0 este ataque se aprovecha de una debilidad en el manejo de un tipo de relleno del cifrado, permitiendo a un atacante, bajo ciertas condiciones, descifrar la información poco a poco.

Conclusión Profesional: Hoy en día, cualquier servicio que aun soporte SSL 2.0 o SSL 3.0 es considerado un grave riesgo de . de seguridad. Un admin debe asegurarse de que estos protocolos esten completamente deshabilitados.

TLS 1.0 y TLS 1.1

El Problema: Con el tiempo, se descubrieron vulnerabilidades significativas, como el ataque BEAST (Browser Exploit Against SSL/TLS) que afectaba a TLS 1.0 y permitía a un atacante recuperar información de las cookies del usuario. Aunque se crearon mitigaciones no resolvieron el problema fundamental

A partir de 2020, los principales navegadores como chrome, Firefox, safari y Edge dejaron de soportar TLS 1.0 y TLS 1.1

TLS 1.2 y TLS 1.3

TLS 1.2 introdujo un conjunto de mejoras que lo hicieron mucho más robusto.

TLS 1.3 es la versión más reciente y ofrece mayor velocidad y seguridad al simplificar la negociación de la conexión (el "handshake") y elimina todos los algoritmos y cifrados inseguros

Conclusión Profesional: Cualquier servidor moderno debe estar configurado para usar al menos TLS 1.3 y preferiblemente TLS 1.3