Práctica 2. Instalación y configuración de un servicio de correo seguro.

La correcta configuración de los servicios de correo electrónico SMTP, IMAP y POP3 utilizando tecnologías como SPF, DKIM, STARTTLS y SSL/TLS es fundamental en la actualidad debido a la necesidad de garantizar la seguridad, la autenticidad y la confidencialidad de las comunicaciones por correo electrónico.

En primer lugar, el SPF (Sender Policy Framework) ayuda a prevenir el correo electrónico no autorizado al verificar si el servidor de correo saliente está autorizado para enviar mensajes en nombre del dominio. Al configurar correctamente el SPF, se evita que los spammers falsifiquen la dirección de correo electrónico del remitente y se reduce la probabilidad de que los correos electrónicos legítimos sean marcados como spam.

Por otro lado, el DKIM (DomainKeys Identified Mail) permite verificar la autenticidad del remitente y la integridad del mensaje mediante la firma digital. Al utilizar DKIM, se genera una firma digital única para cada mensaje saliente, lo que garantiza que no haya sido modificado durante la transmisión y que proviene del dominio que afirma ser.

Además, la implementación de STARTTLS proporciona una capa de cifrado para las conexiones SMTP, IMAP y POP3, lo que asegura que los datos transmitidos entre los servidores de correo sean confidenciales y no puedan ser interceptados o leídos por terceros no autorizados.

Por último, el uso de SSL/TLS (Secure Sockets Layer/Transport Layer Security) brinda una capa de seguridad adicional al cifrar la comunicación entre el cliente de correo y el servidor. Esto protege la información sensible, como las contraseñas y los datos de los correos electrónicos, frente a posibles ataques de interceptación o robo de información.

Un buen perito forense debe poseer conocimientos sólidos en la instalación y configuración de servicios de correo electrónico seguro, ya que esto le permite comprender a fondo los métodos de protección y las posibles vulnerabilidades que pueden afectar al servicio. Al tener la capacidad de implementar y configurar adecuadamente tecnologías como SPF, DKIM, STARTTLS y SSL/TLS, el perito forense adquiere una comprensión profunda de los mecanismos de seguridad y autenticación utilizados en el correo electrónico.

La habilidad de instalar y configurar estos servicios brinda al perito forense una visión clara de las medidas de protección implementadas y les permite evaluar las posibles debilidades que podrían ser explotadas en un escenario de ataque o investigación forense. Al tener un conocimiento exhaustivo de las configuraciones seguras, el perito forense puede identificar rápidamente cualquier configuración incorrecta o deficiente que pueda haber sido aprovechada por un atacante.

Además, la capacidad de comprender y utilizar estas tecnologías también permite al perito forense recuperar y analizar metadatos importantes, como las cabeceras de los correos electrónicos, que pueden proporcionar valiosa información sobre la autenticidad, la ruta de transmisión y los posibles puntos de vulnerabilidad.

En conclusión, el dominio de la instalación y configuración de servicios de correo electrónico seguro es esencial para un perito forense, ya que les proporciona un profundo conocimiento de los métodos de protección y vulnerabilidades que pueden afectar a estos servicios. Esto les permite realizar investigaciones forenses exhaustivas, identificar posibles brechas de seguridad y presentar pruebas sólidas en casos legales relacionados con el correo electrónico.

Objetivos:

- Tomar conciencia de todos los aspectos de seguridad importantes que tienen que ver con el correo electrónico.
- Aprender a instalar y configurar servicios de email que ayudará a tener un conocimiento más profundo en este ámbito de cara a la realización de periciales forenses de emails.

Materiales

- Gestión de un dominio DNS
- Conexión a Internet con posiblidad de apertura de puertos (NO CGNAT)
- Un sistema operativo donde instalar los servicios de correo electrónico: SMTP, POP3 e IMAP
- Un cliente de correo tipo Thunderbird y outlook.

Se pide:

1) Accede a tu dominio y configura los registros MX, SPF y DKIM en el servidor DNS. Recuerda que los registros MX son necesarios para que los servidores de correo electrónico sepan a qué dirección IP deben enviar los correos electrónicos destinados al dominio. Para ello, se debe configurar el registro MX en el servidor DNS del dominio.

   El registro SPF se utiliza para indicar cuáles son los servidores de correo electrónico autorizados para enviar correos electrónicos en nombre del dominio.

   Finalmente, el registro DKIM se utiliza para autenticar los correos electrónicos enviados desde el dominio, lo que ayuda a evitar que los correos electrónicos legítimos sean clasificados como spam. Puedes hacer uso de alguna utilidad tipo DKIM Record Generator

2) Instala los servicios de correo electrónico SMTP e IMAP y POP3. Tienes libertad para elegir el software: en Windows puedes usar hMailServer, en Linux los servicios Postfix y Dovecot, un contenedor docker o el servicio Mail Server si dispones de un NAS marca Synology u otra configuración en la que tengas interés. Que no se te olvide:

- Definir el dominio
- Crear usuarios
- Habilitar las modalidades seguras (SSL/STARTTLS) de los protocolos SMTP, POP e IMAP.
- Habilitar una cuenta de smtp relay.
- Establecer la clave privada DKIM encargada de la firma de los correos.

3) Abre en tu router los puertos entrantes correspondientes a los servicios SMTP, POP e IMAP. Es importante asegurarse de que estos puertos estén abiertos para que el servidor de correo electrónico pueda recibir correos electrónicos y que los usuarios puedan acceder a sus cuentas de correo electrónico a través de los clientes de correo electrónico.

Tipo	Número de puerto	Protocolo
IMAP	143	TCP
IMAP sobre SSL/TLS	993	TCP
POP3	110	TCP
POP3 sobre SSL/TLS	995	TCP
SMTP	25	TCP
SMTP-SSL	465	TCP
SMTP-TLS	587	TCP

4) Instala el cliente de correo Thunderbird u otro similar y configura una cuenta de tu dominio donde puedas comprobar que efectivamente tus correos pueden ser enviados y recibidos.