📁 LPIC-2 / 📨 Examen 211 - Servicios de Correo Electrónico

211.3 Filtrar correo electrónico

Teoría

El filtrado de correo electrónico es el proceso de examinar los correos para identificar y tomar acciones sobre mensajes no deseados (spam) o maliciosos (virus, malware).

Tipos Comunes de Filtrado:

- **Filtrado de Contenido/Spam:** Analiza el texto del cuerpo, los encabezados y otras características del mensaje para determinar si es spam. Utiliza reglas, heurística y a veces listas negras/blancas basadas en contenido.
- **Escaneo Antivirus:** Busca patrones conocidos de malware en archivos adjuntos o en el cuerpo del mensaje.
- **Filtrado Basado en Conexión/Dirección:** Bloquea o permite correo basado en la dirección IP del remitente, el dominio, la dirección de correo del remitente/destinatario, o usando técnicas como Greylisting.

Herramientas Comunes de Filtrado en Linux:

1. **SpamAssassin:**
    - Una herramienta de código abierto ampliamente utilizada para identificar spam mediante una variedad de pruebas heurísticas y estadísticas sobre encabezados y cuerpo del correo. Asigna una puntuación de "spam" a cada mensaje; si la puntuación excede un umbral, se marca como spam (típicamente modificando los encabezados del correo).
    - **Componentes:**
        - `spamd`: El demonio de SpamAssassin, que corre en segundo plano para procesar solicitudes de escaneo de forma eficiente.
        - `spamc`: Un cliente ligero que se comunica con `spamd` para escanear un correo.
    - **Actualizaciones:** Las reglas de SpamAssassin se actualizan regularmente para combatir nuevas técnicas de spam usando el comando `sa-update`.
    - **Configuración:** Archivos en `/etc/mail/spamassassin/` y reglas de usuario en `~/.spamassassin/`.
    - **Paquete:** `spamassassin` (estándar).
2. **ClamAV:**
    - Un motor antivirus de código abierto, muy común para escanear correo y archivos en servidores Linux.
    - **Componentes:**
        - `clamd`: El demonio de ClamAV, que corre en segundo plano para procesar solicitudes de escaneo.

    - `freshclam`: Utilidad para descargar y actualizar la base de datos de definiciones de virus.
    - `clamscan`: Cliente de línea de comandos para escanear archivos manualmente.
- **Actualizaciones:** La base de datos de virus se actualiza usando el comando `freshclam`. Esto es crucial para detectar amenazas recientes.
- **Configuración:** Archivos en `/etc/clamav/`.
- **Base de Datos de Virus:** Almacenada típicamente en `/var/lib/clamav/` (con permisos para el usuario de `clamd`).
- **Paquetes:** `clamav` (utilidades) y `clamav-daemon` (el demonio `clamd`). Estándar en ambas ramas.

Integración de Filtros con el MTA (Postfix):

Las herramientas de filtrado necesitan integrarse con el MTA para procesar todos los correos. Esto se hace configurando el MTA para pasar el correo a través de los filtros en puntos específicos del flujo.

- **Filtro de Contenido (Pipe):** Un método común con Postfix es usar la directiva `content_filter`. Postfix "inyecta" el correo a un programa especificado (a menudo un script "wrapper" que llama a `spamc` o `clamscan`) y luego procesa la salida del programa.
    - Se configura en `main.cf` (ej: `content_filter = scan:localhost:10024`, donde `scan` es un servicio definido en `master.cf`).
    - En `master.cf`, se define el servicio `scan` para que use un programa (ej: `smtp-amavis`, `sendmail -G -L -o ...`) que a su vez interactúa con SpamAssassin y ClamAV. La integración completa con ambos a menudo implica un "wrapper" como `amavisd-new` (que es otro paquete y servicio) que coordina las llamadas a SpamAssassin y ClamAV.
- **Milter (Mail Filter API):** Postfix (y Sendmail) soportan Milter, que permite a los programas interactuar con la sesión SMTP en varias etapas (conexión, HELO, remitente, destinatario, datos - antes de la cola). SpamAssassin y ClamAV (a través de `clamav-milter`) pueden integrarse como Milters. Se configura en `main.cf` (ej: `smtpd_milters = unix:/<ruta_socket_milter>`).

Funciones de Filtrado Integradas en Postfix:

Postfix también tiene capacidades de filtrado básicas integradas sin necesidad de herramientas externas:

- **Listas de Control de Acceso (ACLs):** Usando directivas como `smtpd_recipient_restrictions`, `smtpd_sender_restrictions`, `smtpd_client_restrictions`, `smtpd_helo_restrictions`. Permiten `allow`/`reject` basado en listas negras/blancas de dominios, direcciones IP, patrones, etc.

(Ej: `reject_rbl_client <lista_rbl>` para rechazar remitentes listados en bases de datos de listas negras de DNS - RBLs).
- **Verificaciones de Encabezados y Cuerpo:** Usando `header_checks` y `body_checks` para rechazar o modificar correos basados en patrones (expresiones regulares) en los encabezados o el cuerpo.

Gestión de Herramientas de Filtrado:

- **Actualizaciones:** Mantener actualizadas las reglas de SpamAssassin (`sa-update`) y las definiciones de virus de ClamAV (`freshclam`) es crítico para una detección efectiva. Esto debe programarse (cron o systemd timers).
- **Monitorización:** Revisar los logs de SpamAssassin y ClamAV (`/var/log/mail.log`, `/var/log/clamav/clamav.log` o journald) para ver si los filtros están funcionando, si hay errores, o si están detectando spam/virus.
- **Servicios:** Asegurarse de que los demonios `spamd` y `clamd` estén corriendo si se usan en modo cliente/servidor (`spamc`/`clamscan` llaman a los demonios).

Diferencias Debian vs. Red Hat (Filtrado):

- Los nombres de paquetes para SpamAssassin (`spamassassin`) y ClamAV (`clamav`, `clamav-daemon`) son generalmente estándar.
- Las ubicaciones de los archivos de configuración (`/etc/mail/spamassassin/`, `/etc/clamav/`) y las bases de datos de virus (`/var/lib/clamav/`) son en su mayoría estándar.
- La integración específica con Postfix (cómo modificar `main.cf` y `master.cf`) puede tener variaciones sutiles en la configuración de ejemplo o las rutas de scripts/sockets, aunque el concepto de usar `content_filter` o `milter` es el mismo.
- Las herramientas de ayuda para la integración (como `amavisd-new`) pueden tener nombres de paquetes y configuraciones específicas de distribución.