# LINUX WEEK PUCP 2006

## Control Antivirus y Antispam en sistemas Linux

Ing. Genghis Ríos Kruger

# Agenda

- Virus en Linux
- Spam
- Programas disponibles
- Correo Electrónico
- Escaneo del Correo
- Programa Filterman

# Los Virus

- La gran mayoría de virus que existe son básicamente para el sistema Windows.
- Ejemplo: Con F-Prot se obtienen los siguientes resultados para sistemas Unix y Windows

```
DOS/Windows: 109202 viruses and 61558 Trojans
Word/Excel: 8543 viruses and Trojans
Unix shell: 405 viruses and Trojans
Unix: 432 viruses and Trojans
```

# Los Virus

- Sin embargo en un servidor Linux podemos guardar archivos que provengan de sistemas con Windows.
- Un servidor que ofrezca servicio de correo procesará mensajes con archivos también.

# El Spam

- Según Wikipedia: El Spam es el correo no deseado **Spam** son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

# El Spam

- Según estadísticas el 80% del correo que circula en Internet es Spam.
- Del lado del usuario consume tiempo estar borrando estos mensajes.
- Del lado del servidor se consume tiempo de proceso y espacio de disco.
- Del lado de la red se consume ancho de banda.
- Del lado del administrador un gran dolor de cabeza para combatirlo.

# El Spam

- Los *spammers* (individuos o empresas que envían spam) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren internet en busca de direcciones.

# El Spam

- Los servidores de correo mal configurados son aprovechados también por los *spammer*. En concreto los que están configurados como Open Relay. Estos no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos.

# Precauciones

- Modificar la dirección para evitar el rastreo automático. Por ejemplo, cambiar "nombre@dominio.com" por "nombre (ARROBA) dominio (PUNTO) com", "nombre@dominioNOSPAM.com, quita NOSPAM" o "n0mbre@d0mini0.c0m (sustituir los ceros por oes)". Ayuda pero no es 100% efectivo.

- No hacer envíos a amigos o colaboradores en los que aparezcan muchas direcciones y, si se hace, usar Bcc (o CCO) para que no sean visibles las demás direcciones.

- No enviar nunca mensajes al *spammer*, aunque prometan dejar de enviar spam si se les pide

# Programas Antivirus para Linux

- Prácticamente todas las grandes empresas antivirus brindan soluciones bajo Linux. Ejemplos: **Mcafee, Panda, F-Prot, Kaspersky, BitDefender**, **Trend Micro** incluso productos nacionales como **Hacker** y **PER**.
- Soluciones libres hay pocas, la mejor de todas es **Clamav.**
- No todos ofrecen escaneo en tiempo real. En dicho caso funcionan con un kernel en particular.

# Antivirus en Linux

- No todos los antivirus tienen la misma velocidad y capacidad de detección
- Si tenemos un sistema con alto tráfico de archivos necesitamos un antivirus que genera la menor carga y que sea lo más rápido posible. Balancear ésta decisión junto con la capacidad de detección y actualización frente a nuevos virus.

# Antivirus en Linux

- Para aumentar la velocidad de detección y disminuir el nivel de carga es preferible usar aquellos antivirus que permiten ejecución en background, como un servicio del sistema.

# Antivirus en Linux

- **Mcafee**: Muy buena capacidad de detección, pero elevada carga al momento de su ejecución y lentitud. Propietario.
- **F-Prot:** Buena capacidad de detección, elevada velocidad, mínima carga, ejecución como demonio. Propietario, con costo, pero gratis en su versión workstation para uso personal.
- **Clamav:** Elevada velocidad, buena capacidad de detección, ejecución como demonio, constante actualización, y es libre !!!!!

# Antispam en Linux

- Existen también varias soluciones, pero la más difundida es **Spamassassin**
- Se puede ejecutar en background (como demonio) lo que ayuda a acelerar su ejecución al momento del escaneo
- Sin embargo es de lejos más pesado que cualquier antivirus debido a las sofisticadas técnicas que emplea para detección de spam, basados en algoritmos bayesianos y técnicas estadísticas.

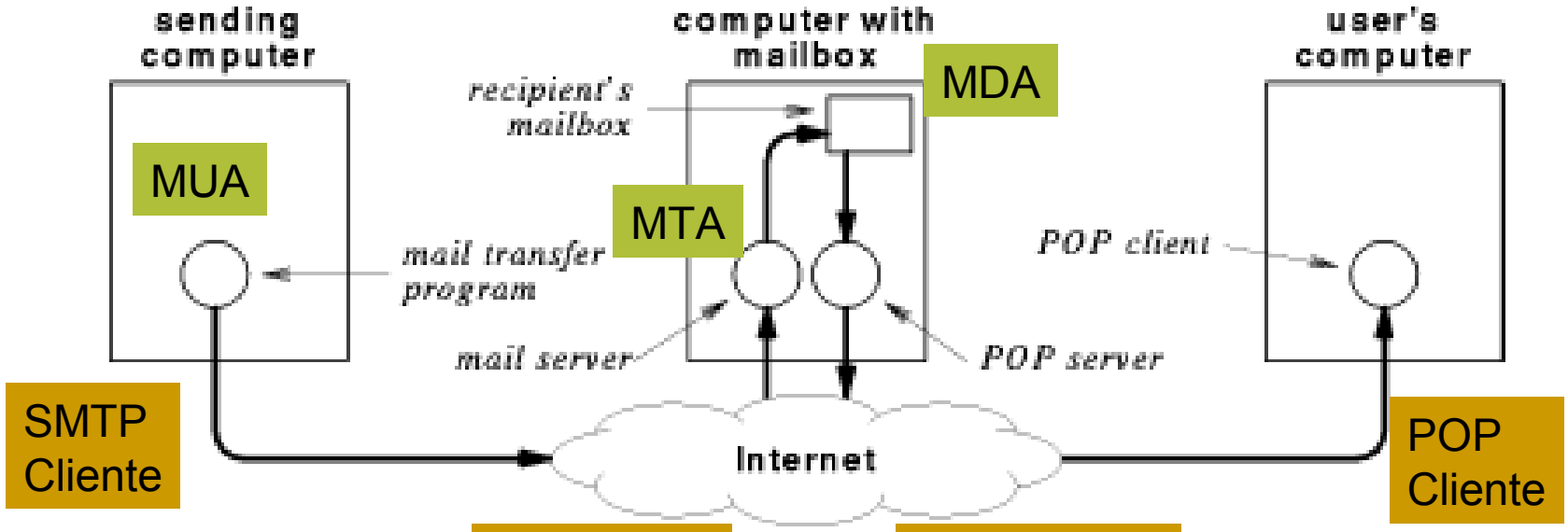
# Correo Electrónico

- Un sistema de correo electrónico consta de los siguiente servicios:
- **SMTP**: Para envío del correo.
- **POP/IMAP**: Para descarga del correo. IMAP adicionalmente permite crear carpetas en el servidor.

# Correo Electrónico

- Al cliente de correo SMTP se le llama **MUA** (Mail User Agent), es el que compone el mensaje.
- Al Servidor SMTP se le llama **MTA** (Mail Transfer Agent), recibe el mensaje desde el cliente y lo reenvía hacia otro MTA de ser necesario.
- Cuando el MTA recibe un mensaje no lo almacena directamente en el buzón del usuario sino que pasa a cola.
- Existe un último mensaje que recibe el mensaje de la cola y lo deposita en el buzón del usuario, se llama **MDA** (Mail Delivery Agent)

# Correo Electrónico



# Correo Electrónico

- **MUA:** *Thunderbird, Evolution, Pine, Mutt*
- **MTA:** *Postfix, Sendmail*
- **MDA:** *Procmail, Maildrop*

- Un MTA puede recibir un único mensaje que vaya dirigido a ***N*** destinatarios en el servidor, entonces el MDA se ejecuta ***N*** veces.
- Un escaneo será más eficiente cuando se lanza desde el MTA filtrando el mensaje.

# Escaneo del Correo Electrónico

- El correo electrónico procesa mensajes que pueden contener archivos con virus o spam.
- Dado que el 80% del correo que circula en Internet es Spam es preferible escanear primero el mensaje con el antispam para descartarlo lo antes posible.
- **¿Cómo enlazamos el MTA con los programa antivirus y antispam?**

# Escaneo del Correo Electrónico

- Para luchar contra los virus ayuda mucho filtrar directamente desde el MTA archivos con extensión exe, com, bat, pif, etc. Pero muchos virus vienen como zip. Contra el Spam se pueden filtrar direcciones email, lo cual se puede hacer también desd el MDA para un usuario en particular. Pero esto no es suficiente.
- Existen diversas soluciones para enlazar programas antivirus y antispam con MTAs como Postfix o Sendmail.
- Los más conocidos son:
  - **Amavis**
  - **MailScanner**

# Escaneo del Correo Electrónico

- **Amavis:** El más popular, pero de difícil de configurar (al menos para los novatos :b). La personalización es algo dura tambien.
- **Mailscanner:** Instalación más sencilla, crea su propio sistema de colas para procesar los mensajes.

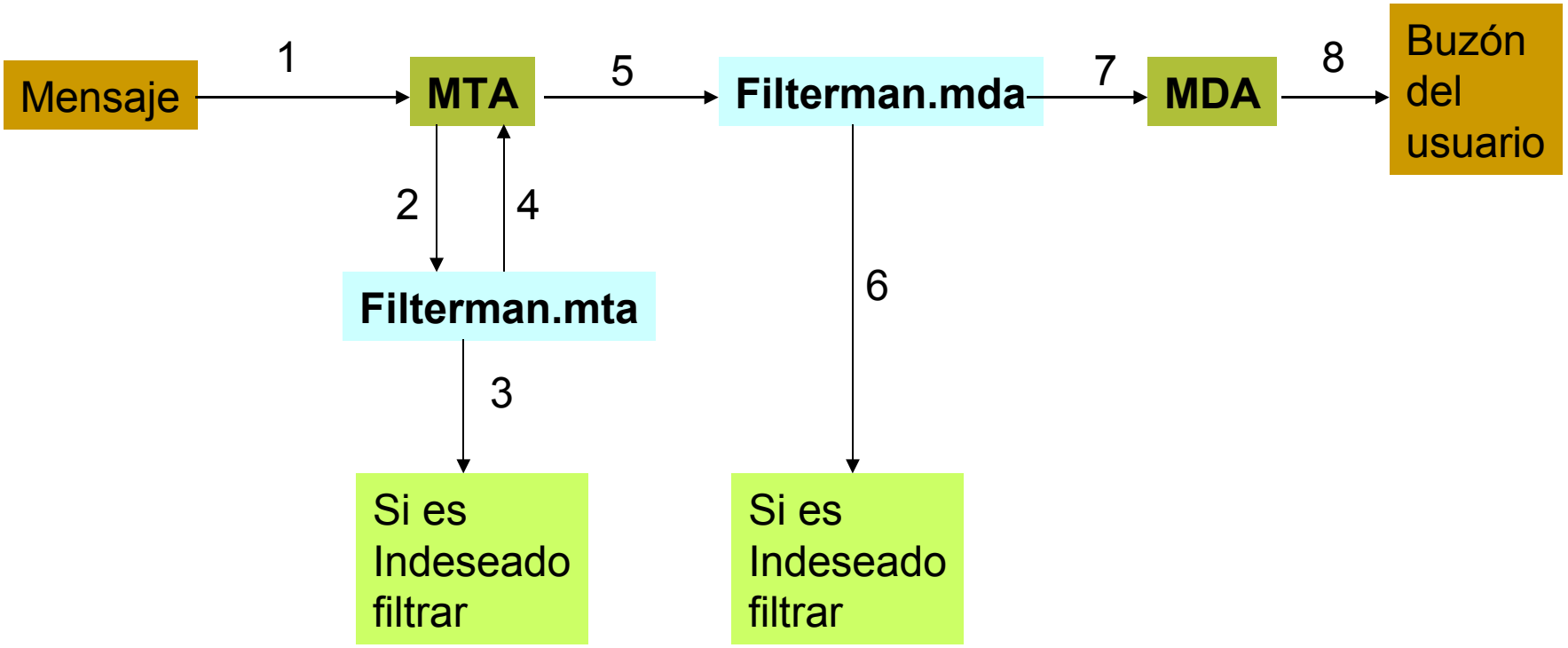
# Escaneo del Correo Electrónico

- **No tiene sentido responder al remitente que el mensaje ha sido rechazado !!!**
- Dado que el 80% del correo de Internet es spam es una pérdida de tiempo activar respuestas automáticas a estos mensajes indeseados, sin embargo gran porcentaje de los administradores de correo lo activan por ignorancia o por usar la configuración por default.

# Filterman

- El programa Filterman permite enlazar tanto un MTA como un MDA con programas antivirus y antispam.
- El enlace con el MTA lo hace el programa **filterman.mta**
- El enlace con el MDA lo hace el programa **filterman.mda**

# Filterman


Mensaje
1
MTA
5
Filterman.mda
7
MDA
8
Buzón del usuario
2
4
Filterman.mta
3
6
Si es Indeseado filtrar
Si es Indeseado filtrar

# Filterman

- **filterman.mta** está más orientado a ejecutar los programas antivirus como f-prot, mcafee o antispam como clamav para escanear el mensaje de correo.
- **filterman.mda** está más orientado a controlar las respuestas automáticas de un usuario (*"me fuí de vacaciones"*), a filtrar mensajes de direcciones email indeseadas, y a controlar la cuota del usuario según el grupo, problema que actualmente no resuelven soluciones como Amavis o Mailscanner.
- Ambos se pueden instalar por separado.

# Filterman

- Filterman trabaja básicamente con **Postfix** como MTA y **procmail** como MDA.
- Es de fácil instalación.
- Muy fácil de personalizar por ser de código pequeño.
- Soporta mailboxes en formato mbox y maildir.
- Escrito en *shell script* pero con mínima carga de ejecución. **La mayor carga la generan los programas antivirus y sobre todo los antispam**.
- A publicarse en Sourceforge en unos días.

# Consultas?