

## El Día a Día del Administrador de Sistemas: P3Scan

## LIBRE DE VIRUS

La misión de un gateway SMTP o de un servidor directamente conectado a él es analizar el correo en busca de virus. En la columna de este mes, Charly decide cambiar de lado esta protección, es decir, colocarla en las conexiones del cliente con sus servidores SMTP o POP. **POR CHARLY KÜHNAST**

**P**3Scan [1] es un proxy para el correo electrónico que se monta delante de los servicios SMTP y POP3 y que acepta conexiones de clientes que quieren recoger el correo o librarse de él. Se encarga de reenviar los comandos de los clientes y de comprobar los correos en busca de contenido malicioso antes de pasarlos. P3Scan evita dependencias raras y se basa en las bibliotecas *pcre-devel*, que la mayoría de las distribuciones probablemente contengan.

Por supuesto, P3Scan debe confiar en el software antivirus. Yo elegí ClamAV, pero también funcionará con F-Prot, F-Secure, Kaspersky y probablemente otros productos que se puedan utilizar en la línea de comandos. P3Scan puede integrar SpamAssassin y DSPAM, permitiendo eliminar del correo publicidad no solicitada.

Iptables proporciona a los administradores la capacidad de utilizar P3Scan como un proxy transparente para el correo. Los usuarios no notan la existencia del programa, por lo menos mientras el correo entrante esté limpio. Se podría instalar en un router Linux fácilmente. P3Scan funcionó en un puerto no privilegiado, por defecto el 8110, utilizando iptables para enviar todas las conexiones POP3 al puerto solicitado:

```
iptables -t nat -I ➤
PREROUTING ! -i eth0 ➤
-p tcp -s 192.168.1.0/24 ➤
-dport 110 -j REDIRECT ➤
-to-ports 8110
```

## SYSADMIN

Zeus.....64

Mantén en línea sitios web sobrecargados con este balanceador de carga basado en Linux.

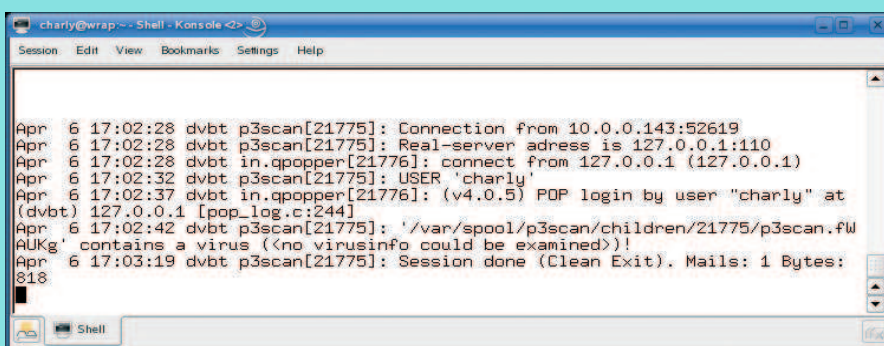


Figura 1: Protocolo P3Scan para un correo entrante. Afortunadamente, éste está libre de virus.

Tras hacer esto, aceptará conexiones POP3, pasando todos los comandos POP, tales como RETR, DELE, etc., a la tarjeta del servidor y capturando los emails legítimos de éste. También pasa el correo por el antivirus y si es necesario, por el filtro antispam.

## Configuración

P3Scan se controla con el fichero */etc/p3scan/p3scan.conf*. Las siguientes entradas son importantes:

*targetip*: Si quiere utilizar P3Scan como un proxy transparente, debe introducir *0.0.0.0*. Si no, introduzca la dirección IP de un servidor “real” donde P3Scan reenviará las conexiones de los clientes.

*bytesfree* = < byte >: Necesita al menos *bytes* de espacio libre en disco; de lo contrario P3Scan no funcionará. Tenga en cuenta que el programa genera un cierto número de procesos hijos (por defecto: 10); el peor de los casos se dará cuando todos ellos necesitan manejar datos adjuntos de gran tamaño a la vez.

*scanner* = < comando >: Aquí se introduce el comando que ejecutará el antivirus. Como yo utilizo ClamAV, mi línea de comandos será como ésta:

```
scanner = /usr/bin/clamscan ➤
-no-summary
```

*viruscode* = : P3Scan evalúa el código que devuelve el antivirus para determinar si el correo está infectado o limpio. Normalmente, el antivirus devolverá un valor de 0 si el mensaje está limpio y 1 si encuentra un virus. Algunos antivirus utilizan códigos adicionales. Para indicarle a P3Scan que evalúe estos códigos, se necesitará una línea adicional en el fichero. Si el antivirus devuelve un valor de 1, 5 ó 13 para “¡Virus detectado!”, la línea será *viruscode* = 1, 5, 13. El mismo principio se aplica a los códigos devueltos como 0 que indica “No se ha detectado virus”. Entonces la línea comenzará con *goodcode* = .

*overwrite* = */usr/bin/p3pmail*: Esta línea elimina los correos HTML. Evita que los clientes carguen autónomamente imágenes o similares mientras se lee el correo. Esto podría ser peligroso. También le permite conocer a los spammers que el mensaje ha llegado y se ha abierto. ■

## RECURSOS

[1] P3Scan: <http://p3scan.sourceforge.net>