¿Cuál es formato del mbox de UNIX (buzón)?

Contenido

Introducción

Este documento describe el formato del buzón de Unix (mbox) y cómo se relaciona para utilizar en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

¿Cuál es formato del mbox de UNIX (buzón)?

El formato del mbox de UNIX es utilizado por AsyncOS cuando los mensajes están archivados y abrió una sesión la acción del log() del filtro del mensaje. El “mensaje del archivo” es una opción de configuración adicional para el Anit-Spam de Ironport (IPA), el contra virus (Sophos y McAfee), la protección avanzada de Malware (AMP), y Graymail en el ESA.

El formato de Mbox es (es decir,) un formato de archivo no binario ASCII-formatado que puede contener cero o más mensaje del correo. Los mensajes se concatenan en el archivo del mbox y se pueden alzaprimar aparte basaron en las cadenas específicas en el archivo. Este formato es idéntico con el mensaje pues se transfieren entre los gatewayes obedientes del correo del RFC 2821.

Cada mensaje en el formato del mbox comienza con una línea de la cual comience con la cadena “” (caracteres ASCII F, r, o, m, y espacio). “” De las líneas son seguidos por varios más campos: sobre-remitente, fecha, y (opcionalmente) más datos.

El primer campo después del “” de la cadena es el sobre-remitente del mensaje. El dependiente sobre quien la aplicación crea el archivo del mbox, el sobre-remitente pudo ser presente mientras que un buzón o real pudo ser otro carácter o cadena. Lo más comúnmente posible, usted encontrará que “-” (sola rociada del carácter) substituye el sobre-remitente si el sobre-remitente real no es disponible o no sabido. El campo de la fecha insertado por el ESA es en el formato estándar del asctime() de UNIX y es siempre 24 caracteres de largo. En algunos archivos del mbox escritos por las implementaciones NON-AsyncOS, la Más información sigue el sello de fecha. Estos tres campos son separados por un único espacio.

Aquí está un ejemplo de un archivo del mbox con un solo mensaje en él:

```
From Adam@Outside.COM Sun Oct 17 12:03:20 2004
Received: from mail.outside.com (192.35.195.200)
by smtp.alpha.com with ESMTP; 17 Oct 2004 12:03:20 -0700
X-IronPort-AV: i="3.85,147,1094454000";
v="EICAR-AV-Test'0'v";
d="scan'208"; a="86:adNrHT37924848"
X-IronPort-RCPT-TO: alan@mail.example.com
From: Adam@Outside.COM
To: Alan Alpha <Alan@mail.example.COM>
```

```
Subject: Exercise 7a Anti-Virus Scanning
Reply-To: Adam Alpha <adam@outside.com>
Date: Sun, 17 Oct 2004 12:02:39 -0700
MIME-version: 1.0
Content-type: multipart/mixed; boundary="IronPort"

--IronPort
Content-type: text/plain; format=flowed; charset=us-ascii
Content-transfer-encoding: 7bit

Blah blah blah blah blah
Blah blah blah blah blah
Blah blah blah blah blah
...
--IronPort
Content-type: text/plain
Content-transfer-encoding: 7bit
Content-disposition: inline

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*">X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

--IronPort--
```

Cuando se analizan los archivos mbox-formatados, es deseable no leer demasiada semántica en “” de la línea que separa los mensajes. Porque muchas diversas utilidades escriben los archivos del mbox, hay considerable variación en estas líneas. Sin embargo, “” de la línea puede ser utilizado siempre como línea del separador del mensaje para indicar confiablemente que un nuevo mensaje ha comenzado en el archivo del mbox. En todos, hay cerca de 20 formatos sabidos para las cadenas después de “” del separador del mensaje, que generalmente hace muy difícil analizarlo.

Después de que “” de la línea sea un correo electrónico en el formato del RFC 2822, con una serie de encabezados del cuerpo del mensaje seguidas por una línea vacía seguida por el contenido adicional del cuerpo del mensaje.

Para asegurarse de que los mensajes estén separados correctamente, las líneas de las cuales comience con la cadena “” prepended siempre por un solo “**>**”. Diversas diversas variantes de las líneas de la manija de archivos del mbox que comienzan con el “**>**From” diferentemente. En las implementaciones tempranas de las aplicaciones que escribieron los archivos del mbox, estas líneas ellos mismos no fueron citadas. Los archivos del registro de AsyncOS prepend siempre “**>**” a las líneas por las cuales comience con uno o más “**>**” los caracteres seguidos “de”.

Aquí está un ejemplo de un archivo del mbox que contenga un mensaje que tenía líneas de las cuales contenga comenzar ata “”, “**>**From” y “**>>>>**From” en él:

```
From jtrumbo@example1.com Sun Dec 12 12:27:33 2004
X-IronPort-RCPT-TO: trumbo@example1.com
From: jtrumbo@example1.com
To: trumbo@example2.com
Subject: Quote this, if you dare
Date: Sun, 12 Dec 2004 12:28:00 -0700

The following line is just From
>From A From Line

The following line has quoted >From
>>From A >From Line
```

```
The following line has many >>>>From
>>>>>From This line has 4 > characters before From

And this is the last line
```

El extremo de un mensaje en un archivo con formato del mbox es señalado tradicionalmente por una línea vacía. Sin embargo, esto no está siempre presente (aunque AsyncOS lo coloca allí). Cuando se analiza un archivo del mbox-formato, usted debe señalar el extremo de un mensaje por el comienzo de un nuevo mensaje (borre la línea vacía si uno está presente) o para el final del archivo.

Otra variante en el formato del mbox pedido la longitud del mensaje que se señalará en un campo de la “Contenido-longitud” dentro del encabezado del mensaje. Ese formato no utilizó “” de la línea el citar. AsyncOS no utiliza este formato y no inserta un campo de la Contenido-longitud.