



Forense en correo electrónico

Telefónica

EDUCACIÓN DIGITAL

Índice



1 Introducción	3
2 MIME, S/MIME Y SMTP	4
3 Comandos SMTP	4
4 Protocolo extendido SMTP	5

1. Introducción

Hoy en día el correo electrónico es una de las vías de comunicación más utilizada entre las personas en la sociedad actual. Se utiliza como método de intercambio de información interna empresarial, información externa entre individuos, transmisión de documentos y conversaciones de tipo general.

El correo electrónico puede proveer de confidencialidad, autenticación e integridad en los datos, proporcionando al usuario tranquilidad a la hora de utilizar este medio. Dado que este mecanismo ha ido creciendo a lo largo de los últimos años, atacantes maliciosos utilizan también este medio como punto de ataque, debido principalmente al tipo de información que éste puede contener.

A través del correo electrónico se puede propagar malware, producir ataques de robo de información y suplantación de identidad, por citar algunos de los incidentes de seguridad que pueden generar la necesidad de realizar un análisis forense de los protocolos que se relacionen con la transferencia y recepción de correos electrónicos. Esto permitirá al auditor estudiar el origen y contenido de un determinado e-mail para que se pueda identificar varios puntos a tener en cuenta:

- Quién envía el mensaje
- Quién lo recibe
- Fecha a la que se envió
- Contenido del mismo

Existen dos estándares en el desarrollo de correo electrónico. Por un lado, existe el protocolo X400 que fue desarrollado y potenciado en la década de los 80 por varias empresas tecnológicas. Por otro lado, existe el protocolo SMTP (Simple Mail Transfer Protocol) que fue definido también a principios de los 80 por el IETF (Internet Engineering Task Force) y que actualmente está reflejado en los RFC (Request for Comments) 821 y 822.

Este protocolo se ha convertido con el tiempo en uno de los más utilizados en Internet convirtiéndose en un estándar de Internet,

En cuanto a los protocolos de acceso al buzón que acompañan al SMTP, el número de posibilidades varía desde los clásicos POP2 (Post Office Protocol v2), POP3 (Post Office Protocol v3), hasta los IMAP (Internet Message Access Protocol), MAPI (Messaging Application Programming Interface) o los actuales basados en soporte HTTP que se han extendido a medida que crecía la popularidad de la web.



2. MIME, S/MIME Y SMTP

MIME (Multipurpose Internet Mail Extensions) añade una extensión al protocolo SMTP, permitiendo la encapsulación de contenido multimedia dentro de un mensaje SMTP. MIME utiliza BASE64 para codificar y convertir ficheros complejos en datos de tipo ASCII. Está soportado por casi todas las aplicaciones a día de hoy. Se puede consultar los RFC 2045 a 2049.

Una nueva especificación de MIME permite soportar mensajes cifrados y se conoce como S/MIME. Esta especificación está basada en criptografía de clave pública de tipo RSA y ayuda a prevenir la pérdida de confidencialidad por medio de un ataque o una interceptación del envío de mensajes durante el tránsito o almacenamiento de los mismo. Los RFC que especifican S/MIME son el 2311 y 2312.

3. Comandos SMTP

SMTP utiliza un número limitado de comandos que se deben conocer para poder recomponer y seguir los mensajes en una captura de red.

- **HELO:** Lo envía un cliente para identificarse a sí mismo, normalmente con un nombre de dominio.
- **MAIL FRO:** Identifica al remitente del mensaje; se utiliza con el formato MAIL FROM:.
- **RCPT TO:** Identifica a los destinatarios del mensaje; se utiliza con el formato RCPT TO:.
- **DATA:** Lo envía un cliente para iniciar la transferencia del contenido del mensaje.
- **RSET:** Anula toda la transacción del mensaje y restablece el búfer.

- **VRFY:** Comprueba que un buzón está disponible para la entrega de mensajes; por ejemplo, vrfy ted comprueba que hay un buzón para Ted en el servidor local. Este comando está desactivado en las implementaciones de Exchange de manera predeterminada.
- **QUIT:** Termina la sesión.
- **SEND:** Inicia una transacción

En toda transacción de mensajes de correo electrónico es posible conocer la situación del mismo, consultando los códigos de estado referidos a un e-mail. Estos códigos permiten en todo momento saber qué está pasando con el mensaje de correo. Los valores de estado que se utilizan se especifican en el RFC 821 e identifican, desde el estado del servicio, hasta el envío de un comando no válido.

4. Protocolo extendido SMTP

SMTP extendido, llamado ESMTP, es la definición de un conjunto nuevo de extensiones del protocolo SMTP para dotar al servicio de mayor funcionalidad. Este nuevo formato de comandos y funcionalidades se encuentra definido en la RFC 1869. En ella se establece una estructura para todas las extensiones existentes, y marca la pauta para las extensiones futuras. Estas extensiones podrán utilizarlas los clientes de correo electrónico y para ello, podrán consultarle al servidor SMTP si admite dichas extensiones.

Cuando un sistema se conecta a un agente de transmisión de correo, éste puede enviar el comando EHLO, que forma parte del conjunto extendido del protocolo SMTP, en vez del comando original HELO. Si el agente de transmisión de correo soporta SMTP extendido, el servidor responderá con una serie de comandos soportados. Si no soporta ESMTP, el agente mostrará un error de tipo 500, Comando no reconocido, provocando que el agente del cliente sólo trabaje con peticiones de tipo SMTP.

```
root@kali:~# telnet mail.e-katec.com 25
Trying 213.162.209.61...
Connected to mail.e-katec.com.
Escape character is '^]'.
220 vlc1171.hosters.es ESMTP Exim 4.76 Fri, 09 Dec 2016 20:12:59 +0100
HELP
214-Commands supported:
214 AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
AUTH LOGIN
503 AUTH command used when not advertised
EHLO mail.e-katec.com
250-vlc1171.hosters.es Hello 5.40.238.52.static.user.ono.com [5.40.238.52]
250-SIZE 20971520
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
cmZlZW50ZXNAZS1rYXRlYy5jb20=
334 UGFzc3dvcmQ6
```

Imagen 96 SMTP desde Telnet

*eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **smtp** Expression... Clear Apply Guardar

No.	Time	Source	Destination	Protocol	Length	Info
38967	1135.716563	213.162.209.61	192.168.10.177	SMTP	97	S: 503 AUTH command used when not advertised
38972	1147.333402	192.168.10.177	213.162.209.61	SMTP	77	C: EHLO mail.e-katec.com
38974	1147.375500	213.162.209.61	192.168.10.177	SMTP	211	S: 250 vlc1171.hosters.es Hello 5.40.238.52.static.user.ono.com [5.40.238.52] 250 SIZE
38976	1155.398960	192.168.10.177	213.162.209.61	SMTP	66	C: AUTH LOGIN
38978	1155.461060	213.162.209.61	192.168.10.177	SMTP	72	S: 334 VXNlcm5hbnU6
39008	1194.196340	192.168.10.177	213.162.209.61	SMTP	84	C: User: cmZ1ZW50ZXNAZS1rYXRlYy5jb20=
39010	1194.247583	213.162.209.61	192.168.10.177	SMTP	72	S: 334 UGFzc3dvcmQ6

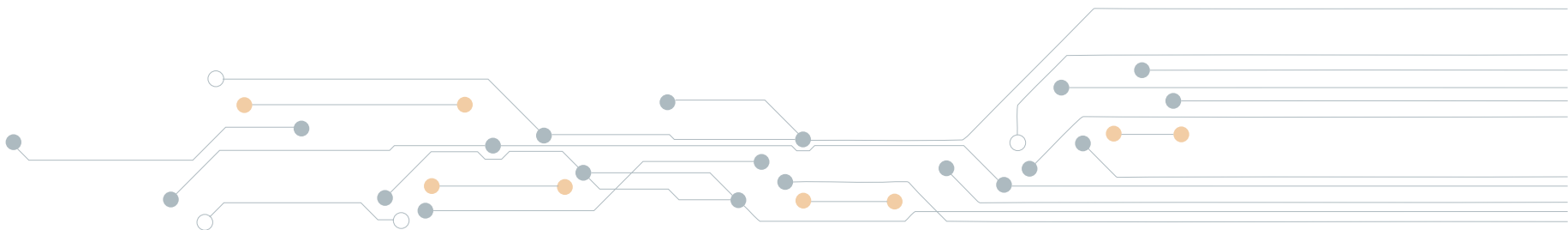
▶ Frame 38972: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_33:6f:3e (00:50:56:33:6f:3e), Dst: Vmware_e6:05:d8 (00:50:56:e6:05:d8)
 ▶ Internet Protocol Version 4, Src: 192.168.10.177 (192.168.10.177), Dst: 213.162.209.61 (213.162.209.61)
 ▶ Transmission Control Protocol, Src Port: 41857 (41857), Dst Port: 25 (25), Seq: 19, Ack: 205, Len: 23
 ▶ Simple Mail Transfer Protocol
 ▶ Command Line: EHLO mail.e-katec.com\r\n

```

0000  00 50 56 e6 05 d8 00 50 56 33 6f 3e 08 00 45 10  .PV...P V3o>..E.
0010  00 3f 29 34 40 00 40 06 9f 3b c0 a8 0a b1 d5 a2  .?)4@.@. .;.....
0020  d1 3d a3 81 00 19 dd 47 95 25 59 de 16 0e 50 18  .=.....G .%Y...P.
0030  72 10 72 6b 00 00 45 48 4c 4f 20 6d 61 69 6c 2e  r.rk..EH LO mail.
0040  65 2d 6b 61 74 65 63 2e 63 6f 6d 0d 0a         e-katec. com..
  
```

File: "/tmp/wireshark_pcapng_eth0_2..." Packets: 42916 · Displayed: 126 (0,3%) · Dropped: 0 (0,0%) Profile: Default

Imagen 97 SMTP desde Wireshark



Telefonica EDUCACIÓN DIGITAL