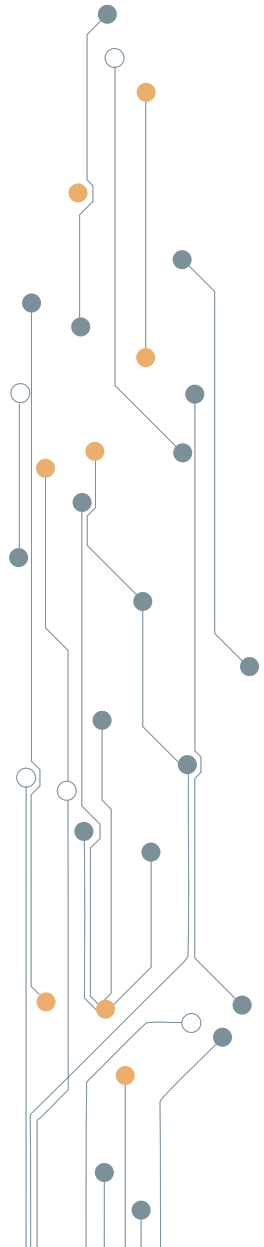
Forense en correo electrónico

Telefónica EDUCACIÓN DIGITAL

Índice



1. Introducción

Hoy en día el correo electrónico es una de las vías de comunicación más utilizada entre las personas en lo 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 trasferencia 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 basad 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 trasmisión 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.

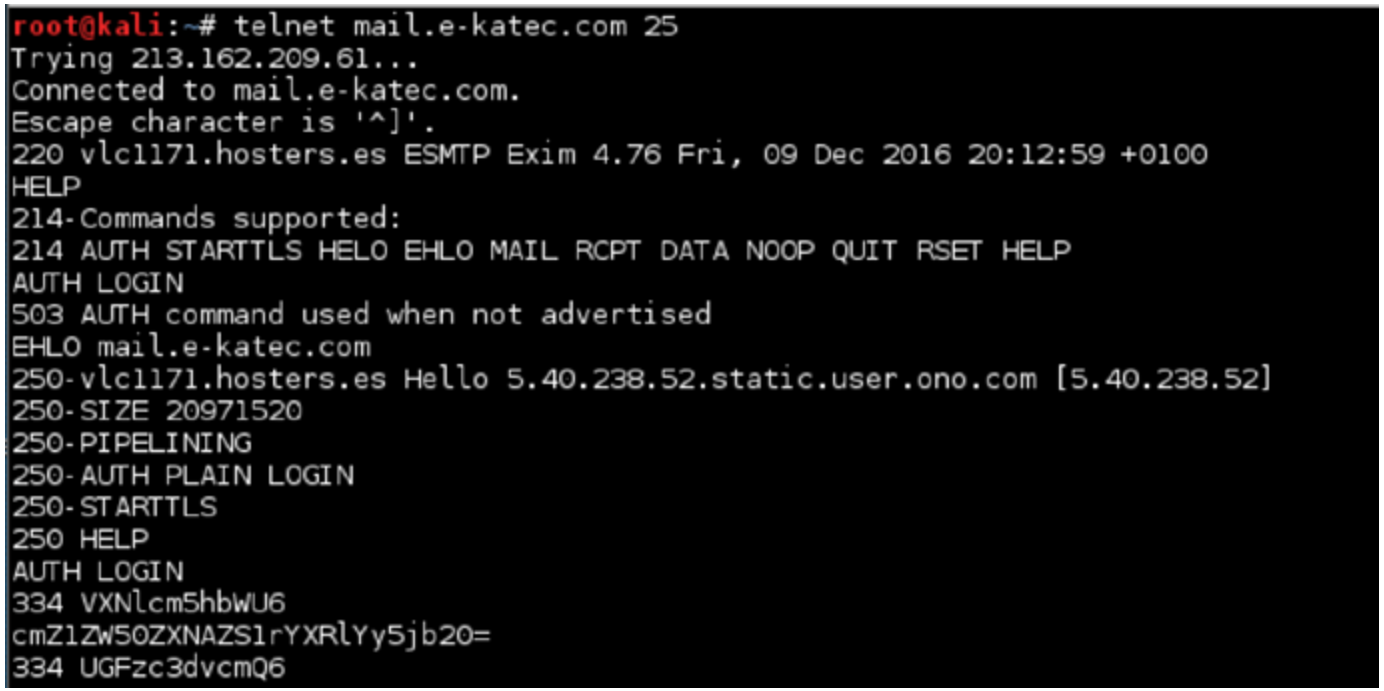


Imagen 96 SMTP desde Telnet

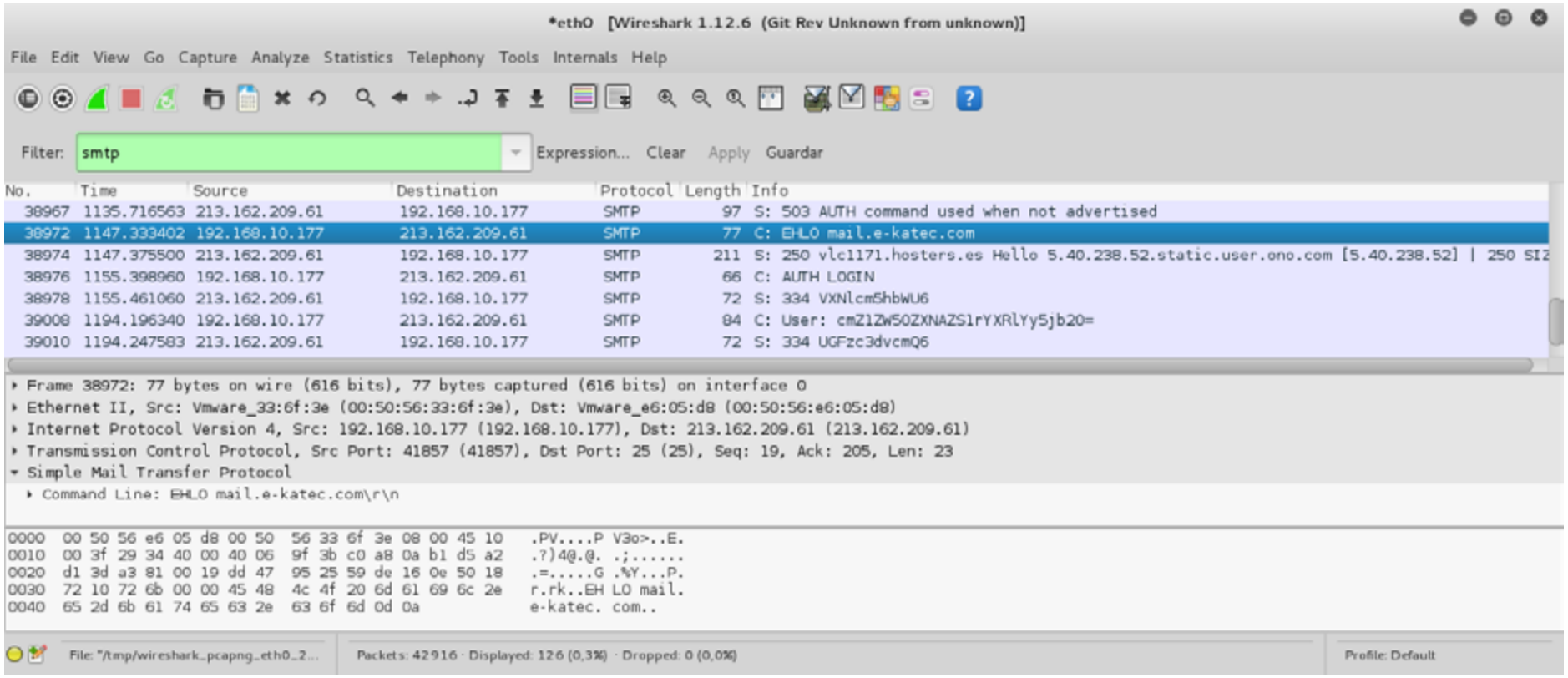


Imagen 97 SMTP desde Wireshark

Telefónica EDUCACIÓN DIGITAL