

Actividad: Protocolos de correo

SMTP y POP3

Conexión manual a los servidores de correo mediante *telnet*

1. *[Instalar y configurar un servidor SMTP y un servidor POP3]*
2. Probar conexión a un servidor SMTP
3. Probar conexión a un servidor POP3
4. Comprobar con *Wireshark* como se transfiere la información

Soporte para SMTP

- Desde una máquina virtual, establecer una conexión con un servidor SMTP mediante Telnet (o netcat)

```
$ telnet smtp.ehu.es 25
```

- Obtener servidores SMTP para un dominio

```
$ dig nombre-dominio MX
```

- Algunos comandos SMTP

```
HELO/EHLO name
```

```
MAIL FROM: emisor
```

```
RCPT TO: receptor
```

```
DATA
```

```
QUIT
```

- Algunas respuestas SMTP

```
220 <servername> Servicio preparado
```

```
421 <servername> Servicio no disponible
```

```
221 <servername> servicio cerrando el canal de transmisión.
```

```
250 Solicitud completada con éxito
```

```
251 Usuario no local; se enviará a <servername>
```

```
354 Introduzca el texto; finalice con solo <CRLF>.<CRLF> en una línea
```

- Ejemplo

```

S: 220 xyz.com Simple Mail Transfer Service Ready
C: EHLO foo.com
S: 250 xyz.com is on the air
C: MAIL FROM:<JQP@bar.com>
S: 250 OK
C: RCPT TO:<Jones@XYZ.COM>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Received: from bar.com by foo.com ; Thu, 21 May 1998
C:      05:33:29 -0700
C: Date: Thu, 21 May 1998 05:33:22 -0700
C: From: John Q. Public <JQP@bar.com>
C: Subject: The Next Meeting of the Board
C: Date: Fri, 21 Nov 1997 09:55:06 -0600
C: Message-ID: <1234@local.machine.example>
C: To: Jones@xyz.com
C:
C: Bill:
C: Podemos quedar el viernes para hablar sobre
C: el viaje de fin de curso.
C:                               John.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

```

Mensaje:
Cabecera + cuerpo

Soporte para POP3

- Desde una máquina virtual, establecer una conexión con un servidor POP3 mediante Telnet.

```
$ telnet mailin.ehu.es 110
```

- Comandos POP3

USER *username*

PASS *password*

LIST

RETR *num-mensaje*

DELE *num-mensaje*

QUIT

- Respuestas POP3

+OK

-ERR

Segurizando SMTP

1. Comprobar si un servidor SMTP admite “*open relay*”
2. Comprobar que extensiones de servicio soporta un servidor SMTP
3. [*Configurar SSL en un servidor SMTP*]
4. Establecer conexión a un servidor SMTP utilizando **STARTTLS**
5. Analizar cabeceras de los mensajes de correo para identificar SMTP aplicado RFC3848

Comprobar con *Wireshark* como se transfiere la información

Soporte

OPEN RELAY Servidor SMTP rechaza el acceso a un usuario que no pertenezca al dominio

ESMTP Empezar sesión con el comando **EHLO**

SMTP + STARTTLS

- Comprobar con Telnet que el servidor acepta conexiones seguras (en el puerto 25)
- Establecer una conexión segura

```
$ openssl s_client -starttls smtp -crlf -connect smtp.ehu.es:25
[-keylogfile mailkeylog.log]
```
- Comenzar intercambio de comandos con el servidor SMTP

Segurizando POP3

1. Comprobar que métodos de autenticación proporciona un servidor POP3
2. Establecer conexión segura con un servidor POP3 utilizando STARTTLS
3. *[Configurar SSL en un servidor POP3]*
4. Establecer conexión segura con un servidor POP3s

Soporte

POP3S

- Establecer sesión segura

```
$ openssl s_client -connect mailin.ehu.es:pop3s
```
- Comenzar intercambio de comandos con el servidor POP3

POP3 + STLS

- Comprobar con Telnet que el servidor acepta conexiones seguras (en el puerto 110)
- Establecer sesión segura

```
$ openssl s_client -starttls pop3 -crlf -connect mailin.ehu.es:110
```
- Comenzar intercambio de comandos con el servidor POP3

Ejercicio: IMAP

- Redactar un informe sobre IMAP que recoja las distintas mejoras en materia de seguridad desarrolladas sobre este protocolo (extensiones, métodos de autenticación...). Analizar cómo realiza el establecimiento de conexiones seguras.