EJERCICIOS SOBRE PROTOCOLOS

Autor: Edward-Ionut, Bunoaica

Ejercicio 1: HTTP

**Parte 1:**

* En este caso he podido observar que se utilizó el método GetAsyncData
* En mi caso se utiliza UserAgent
* Se ha devuelto con 200 y 204

Ejercicio 2: HTTPS

**Parte 1:**

* En mi navegador el que no es seguro me lo muestra sin candado arriba a la izquierda
* Dentro del apartado en HTTPS nos dice que la pagina es segura, en cambio en la que es HTTP nos dice que no lo es
* Porque al no ser una página segura podrían haber grandes vulnerabilidades y ataques a los datos

Ejercicio 3: FTP

**Parte 1:**

* Al instalar filezilla depende de donde queramos pasar o bajar archivos necesitaremos credenciales o no para poder acceder
* Las operaciones de descarga y subida con el servidor se diferencian de las interacciones que hacemos, por ejemplo, para subir archivos el servidor accede a nosotros para poder tomar el archivo y subirlo a la nube, en el caso contrario, al descargar, nosotros accedemos al servidor para poder bajarnos archivos
* Podremos usar varios, pero voy a tratar 3 ejemplos, SFTP mediante SSH, FTPS para transferir archivos de forma segura compatibles con FTP y HTTP O HTTPS para descargar archivos desde la web

Ejercicio 4: SMTP

**Parte 1:**

* He tenido que configurar una cuenta de Gmail y una contraseña, fecha de nacimiento y aceptar la normativa de google.
* Google utiliza un cifrado TLS, esto es importante para que al enviar un correo y llegue a su destinatario se cifre de mientras esté enviándose
* En caso de haber algún fallo en el cifrado SMTP el correo no se enviará y aparecerá un mensaje de error

Ejercicio 5: Comparación entre protocolos

**Parte 1:**

* Es importante usar HTTPS antes que HTTP porque la página web es cifrada y no es vulnerable a ataques y robo de datos
* Es más eficiente usar FTP antes que HTTP a la hora de transferir archivos muy grandes, esto es un ejemplo entre muchos más como por ejemplo mas seguridad o transferencia masiva de archivos

Ejercicio 6: Pensar en la seguridad de los protocolos

**Parte 1:**

* Se podría atacar robando los datos o infectando los sitios con virus, o incluso modificar parámetros
* Usar protocolos de cifrado como HTTPS o SFTP para evitar estos problemas
* Porque al ser una red a la que es visible para la mayoría de dispositivos cercanos pueden ser datos que se roben o sean interceptados por personas ajenas que no queremos que vean nuestros datos