1 El protocolo HTTPS Trabaja sobre el Puerto:

* 443
* 21
* 452
* 462

2 El puerto por defecto del servidor apache es el:

- 8080

- 8082

- 40120

- 80

3 El comando para ver los puertos a la escucha en Linux es:

* netstat -ltn
* netstat -ano
* nslookup
* ifconfig

4 El comando para activar un módulo en apache2 es:

* a2enmod
* a2dismod
* a2ensite
* a2dissite

5 el comando en Windows server para ver los módulos compilados es:

* httpd -l
* http -a
* openssl
* httpd -t

6 el modulo SSl en apache2 recibe el nombre de:

* mod\_ssl.so
* httpd-ssl.conf
* httpd-default.conf
* ssl.so

7 Para ver todos los puertos a la escucha del protocolo TCP en Windows server usamos el comando:

* netstat -a -p TCP
* netstat -a -n -o TCP
* nslookup
* ipconfig

8 El modulo que habilita las carpetas personales de usuarios en Apache2 se llama:

* mod\_userdir.so
* httpd-userdir.conf
* userdir\_mod.so
* http\_userdir.so

9 En Apache2.2 de la versión de Windows Server tenemos activa por defecto la monitorización de Estado del sistema y del propio servidor la url para acceder a verla es:

* ip/server-status
* ip/server-info
* ip/webalizer
* ip/status

10 podemos ver los módulos compilados sin necesidad de usar el comando en la siguiente URL:

* ip/server-status
* ip/server-info
* ip/webalizer
* ip/status

11 En Apache2.2 podemos activar una extensión que nos muestra las estadísticas de USO y RENDIMIENTOS de nuestro servidor podemos acceder a ellas en la siguiente URL:

* ip/server-status
* ip/server-info
* ip/webalizer
* ip/status

12 La autenticación Digest sirven para:

* Es un archivo de autenticación encriptado que sirve para proteger las conexiones a ciertas paginas de nuestro servidor apache2
* Es un archivo encriptado donde se almacena el usuario y la contraseña del administrador del servidor
* La autentificación tipo digest soluciona el problema de la transferencia de contraseñas en claro sin necesidad de usar SSL. Se aplica una función hash a la contraseña antes de ser enviada sobre la red, lo que resulta más seguro que enviarla en texto plano como en la autenticación básica de apoache2.
* Es un archivo donde se guarda el usuario de forma encriptada para asegurar una conexión segura

*\*\* El archivo digest solo almacena la contraseña encriptada por la clave hash del propio sistema no almacena ningún tipo de usuario el usuario viaja por la red sin encriptar, de la propia autenticación se encarga el sistema operativo no el servidor apache2 \*\**