Tarefas

As tarefas propostas son as seguintes.

* Tarefa 2.1. Control de acceso en Linux.
* Tarefa 2.2. Control de acceso en Windows.
* Tarefa 2.3. Autenticación en Linux.
* Tarefa 2.4. Autenticación en Windows.
* Tarefa 2.5. Ficheros .htaccess en Linux.
* Tarefa 2.6. Ficheros .htaccess en Windows.
* Tarefa 2.7. Servidor virtual HTTPS en Linux.
* Tarefa 2.8. Servidor virtual HTTPS en Windows.

Tarefa 2.1. Control de acceso en Linux

Nesta tarefa configuraremos o servidor web en Linux para permitir ou denegar o acceso a distintos directorios en función da IP desde a que se trate de acceder.

Enunciado

* Crea o directorio /var/www/html/proba1 e crea nel un ficheiro HTML co contido que queiras.
* Crea o directorio /var/www/html/proba2 e crea nel un ficheiro HTML co contido que queiras.
* Configura o control de acceso para o directorio proba1 de forma que só poida acceder a el a máquina cliente e non a máquina Windows Server.
* Configura o control de acceso para o directorio proba2 de forma que só poida acceder a el a máquina Windows Server e non a máquina cliente.
* En ambos os casos, proba a listar o directorio raíz do servidor, que sucede?
* Conecta o servidor Apache en Ubuntu en modo ponte (mesma configuración de rede que a da túa máquina real pero sumar 100 ao último byte do teu IP) de forma que sexa visible para todas as máquinas reais da aula e configura o control de acceso para que só poidan acceder dúas máquinas da túa elección a proba1 e outras dúas a proba2.

Tarefa 2.2. Control de acceso en Windows

Nesta tarefa configuraremos o servidor web en Windows para permitir ou denegar o acceso a distintos directorios en función da IP desde a que se trate de acceder.

Enunciado

* Crea o directorio C:\Apache24\htdocs\proba1 e crea nel un ficheiro HTML co contido que queiras.
* Crea o directorio C:\Apache24\htdocs\proba2 e crea nel un ficheiro HTML co contido que queiras.
* Configura o control de acceso para o directorio proba1 de forma que só poida acceder a el a máquina cliente e non a máquina servidor Ubuntu.
* Configura o control de acceso para o directorio proba2 de forma que só poida acceder a el a máquina servidor Ubuntu e non a máquina cliente.
* En ambos os casos, proba a listar o directorio raíz do servidor, que sucede?
* Conecta o servidor Apache en Windows en modo ponte (mesma configuración de rede que a da túa máquina real pero sumar 100 ao último byte do teu IP) de forma que sexa visible para todas as máquinas reais da aula e configura o control de acceso para que só poidan acceder dúas máquinas da túa elección a proba1 e outras dúas a proba2.

Tarefa 2.3. Autenticación en Linux.

Nesta tarefa configuraremos o servidor en Linux para restrinxir o acceso aos recursos a usuarios e grupos.

Enunciado

* Con autenticación HTTP Basic:
* Crea o arquivo de contrasinais con dous usuarios: profesor1 e profesor2.
* Crea o grupo profesores que contén a profesor1 e profesor2.
* Crea o cartafol /var/www/profesor con algún arquivo HTML co contido que prefiras e configura adecuadamente Apache de tres maneiras diferentes:
* Que poida acceder profesor1, pero non profesor2.
* Que poidan acceder ambos profesores.
* Que poidan acceder os membros do grupo profesores.
* Que poida acceder calquera usuario válido.
* Con autenticación HTTP Digest:
* Crea o arquivo de contrasinais con dous usuarios: admin1 e admin2, pertencentes ao dominio xestion.
* Crea o cartafol /var/www/administradores con algún arquivo HTML co contido que prefiras e configura adecuadamente Apache de tres maneiras diferentes:
* Que poida acceder admin1, pero non admin2.
* Que poidan acceder ambos administradores.
* Que poida acceder calquera usuario válido.

Tarefa 2.4. Autenticación en Windows.

Nesta tarefa configuraremos o servidor en Windows para restrinxir o acceso aos recursos a usuarios e grupos.

Enunciado

* Con autenticación HTTP Basic:
* Crea o arquivo de contrasinais con dous usuarios: profesor1 e profesor2.
* Crea o grupo profesores que contén a profesor1 e profesor2.
* Crea o cartafol C:\apache24\htdocs\profesor con algún arquivo HTML co contido que prefiras e configura adecuadamente Apache de tres maneiras diferentes:
* Que poida acceder profesor1, pero non profesor2.
* Que poidan acceder ambos profesores.
* Que poidan acceder os membros do grupo profesores.
* Que poida acceder calquera usuario válido.
* Con autenticación HTTP Digest:
* Crea o arquivo de contrasinais con dous usuarios: admin1 e admin2, pertencentes ao dominio xestion.
* Crea o cartafol C:\apache24\htdocs\administradores con algún arquivo HTML co contido que prefiras e configura adecuadamente Apache de tres maneiras diferentes:
* Que poida acceder admin1, pero non admin2.
* Que poidan acceder ambos administradores.
* Que poida acceder calquera usuario válido.

Tarefa 2.5. Ficheros .htaccess en Linux

Nesta tarefa habilitaremos o uso de ficheiros .htaccess no directorio /home/administrador/propio e probaremos que as directivas incluídas neste arquivo teñen efecto.

Enunciado

* Crea o directorio /home/administrador/propio e asignámoslle un alias para que sexa accesible desde http://192.168.0.1/propio. Creamos o arquivo propio.html nel co contido que queiramos.
* Permite o emprego de ficheiros .htaccess nese directorio para todas as directivas admitidas.
* Crea o ficheiro /home/administrador/propio/.htaccess no que incluiremos a directiva apropiada para que se sirva por defecto o arquivo propio.html e soamente se poida acceder desde a IP da máquina cliente.
* Modifica a directiva AllowOverride para que só poidan sobrescribirse as directivas de control de acceso.
* Modifica a directiva AllowOverride só poidan sobrescribirse as directivas de indexación de directorios.

Tarefa 2.6. Ficheros .htaccess en Windows

Nesta tarefa habilitaremos o uso de ficheiros .htaccess no directorio C:\Users\administrador\propio e probaremos que as directivas incluídas neste arquivo teñen efecto.

Enunciado

* Crea o directorio C:\Users\Administrador\propio e asignámoslle un alias para que sexa accesible desde http://192.168.0.2/propio. Creamos o arquivo propio.html nel co contido que queiramos.
* Permite o emprego de ficheiros .htaccess nese directorio para todas as directivas admitidas.
* Crea o ficheiro C:\Users\Administrador\propio\.htaccess no que incluiremos a directiva apropiada para que se sirva por defecto o arquivo propio.html e soamente se poida acceder desde a IP da máquina cliente.
* Modifica a directiva AllowOverride para que só poidan sobrescribirse as directivas de control de acceso.
* Modifica a directiva AllowOverride só poidan sobrescribirse as directivas de indexación de directorios.

Tarefa 2.7. Servidor virtual HTTPS en Linux.

Nesta tarefa crearemos unha clave privada e un certificado autofirmado que nos servirán para poñer en marcha un sitio virtual HTTPS no servidor Apache en Linux.

Enunciado

* Crea unha clave privada para o sitio.
* Crea un certificado autofirmado para o sitio.
* Configura un sitio virtual HTTPS chamado daw-ssl.com, os seus contidos estarán situados en /var/www/daw-ssl, e actívao.

Tarefa 2.8. Servidor virtual HTTPS en Windows.

Nesta tarefa crearemos unha clave privada e un certificado autofirmado que nos servirán para poñer en marcha un sitio virtual HTTPS no servidor Apache en Windows.

Enunciado

* Crea unha clave privada para o sitio.
* Crea un certificado autofirmado para o sitio.
* Configura un sitio virtual HTTPS chamado daw-ssl.com, os seus contidos estarán situados en C:\Apache24\htdocs\daw-ssl, e actívao.