http – ftp - smtp

Seguridad

José Juan Cerpa Ortega

Seguridad

- Conviene usar firewall.
- También puede ser necesario un proxy a nivel de aplicación.
- Actualizar lo antes posible las aplicaciones para evitar posibles agujeros de seguridad.
- Documentarse bien ya que de una versión a otra puede variar la configuración.

Apache - Seguridad

- Instalación de mayor seguridad.
  - Mover httpd al directorio /sbin
    - Mv /apache/bin/httpd /sbin/httpd
  - Actualizar permisos
    - Chown 0 /sbin/httpd
    - Chgrp 0 /sbin/httpd
    - Chmod 511 /sbin/httpd
  - Colocar el valor de la variable httpd en la nueva ubicación.
    - Vi /apache/bin/apachectl
    - ... httpd = /sbin

Apache - Seguridad

- No es nada seguro que el root ejecute el proceso httpd.
- En las nuevas versiones de apache se han creado usuarios y grupos para esta labor.
  - User Apache ó User Nobody
  - Group Apache ó Group Nogroup
- Tampoco es seguro usar el nombre real de la máquina con la directiva ServerName.
- Si se activa DirectoryIndex en las Directivas contenedoras y no existe la página de inicio indicada por defecto se mostrará el contenido del directorio y eso es peligroso.

Apache - Seguridad

- Port y Listen: Para que escuche por otro puerto.
- Timeout *sg* : Tiempo máximo que mantiene una conexión activa. Evita bloqueos.
- MaxClients *nº* : Límite máximo de clientes conectados a la vez al servidor. Evita ataques de denegación de servicio.
- UserDir *directorio / enable users / disable users* : Habilita las páginas de inicio en usuarios del sistema. Permite el uso del comodín * en las rutas. Deshabilitar root, ftp ...

Apache - Seguridad

- Ej. UserDir disable root ftp
- Ej. UserDir www (/home/*/www)
- El directorio del usuario : user:user 711
- El directorio www : user:apache 750
- Resto de directorios : user:apache 644

Apache - Seguridad

- Control de acceso básico
  - Denegar a muchos
    - <Directory /apache/httpd/ulpgc/html/docs>
    - Order deny, allow
    - deny from all
    - allow from 1.2.3.4 pepe.org clientes.net
    - </Directory>
  - Permitir a muchos
    - <Directory /apache/httpd/ulpgc/html/docs>
    - Order allow, deny
    - Allow from all
    - Deny from 1.2.3.4 pepe.org competencia.net
    - </Directory>

Apache - Seguridad

- LogLevel *tipo* : Apache reconoce 8 niveles de error distintos para determinar la cantidad de información a almacenar.

- ErrorLog */ruta* : Graba información sobre los eventos del servidor en el archivo especificado.

Apache - Seguridad

- LogLevel *Tipo* : Los tipos pueden ser...
  - Debug : Graba todo.
  - Info : Solo mensajes informativos.
  - Notice : Importantes pero no vitales.
  - Warn : Advertencia, quizás importantes.*
  - Error : Fallo. Necesario hacer algo.*
  - Crit : Error grave. Hacer algo rápidamente.
  - Alert : Apocalíptico.
  - Emerg : Emergencia total.

Apache - Seguridad

- TransferLog */ruta* : Graba información acerca de los datos que se transfieren al servidor y desde este.
- LogFormat *"Tipos = %X ..."* nomb: Permite personalizar el formato de los archivos de registro.
- CustomLog /ruta nomb : Crea el fichero de log con el formato especificado con nomb.

Apache - Seguridad

- Registros
  - LogFormat *"Tipos = %X ..."* : Ejemplos de variables para el formato.
    - %A : Dirección IP local
    - %a : Dirección IP remota
    - %f : Ruta del documento solicitado
    - %p : Puerto TCP del que se recibió la solicitud
    - %t : Fecha y hora de la solicitud
    - %T : Tiempo usado para procesar la solicitud
    - %u : Usuario remoto en solicitudes autentificadas
    - %v : Nombre del servidor
    - Ejemplo : LogFormat "hots = %a Fecha = %t Usuario = %u"

Autentificación

- Autentificación Básica (usuario y contraseña) almacenados en un fichero.

```
<Directory /home/empleados>
    Authtype Basic
    AuthName “Ficheros empleados”
    AuthUserFile
  /etc/httpd/usuarios-emp
    Require valid-user
</Directory>
```

Autentificación

- El fichero con los usuarios se crea y se mantiene con htpasswd.
- Ej. Htpasswd –b –c fichero usuario passwd
- Almacenar el fichero de claves en un lugar seguro.
  - - c crea el fichero si este no existe.

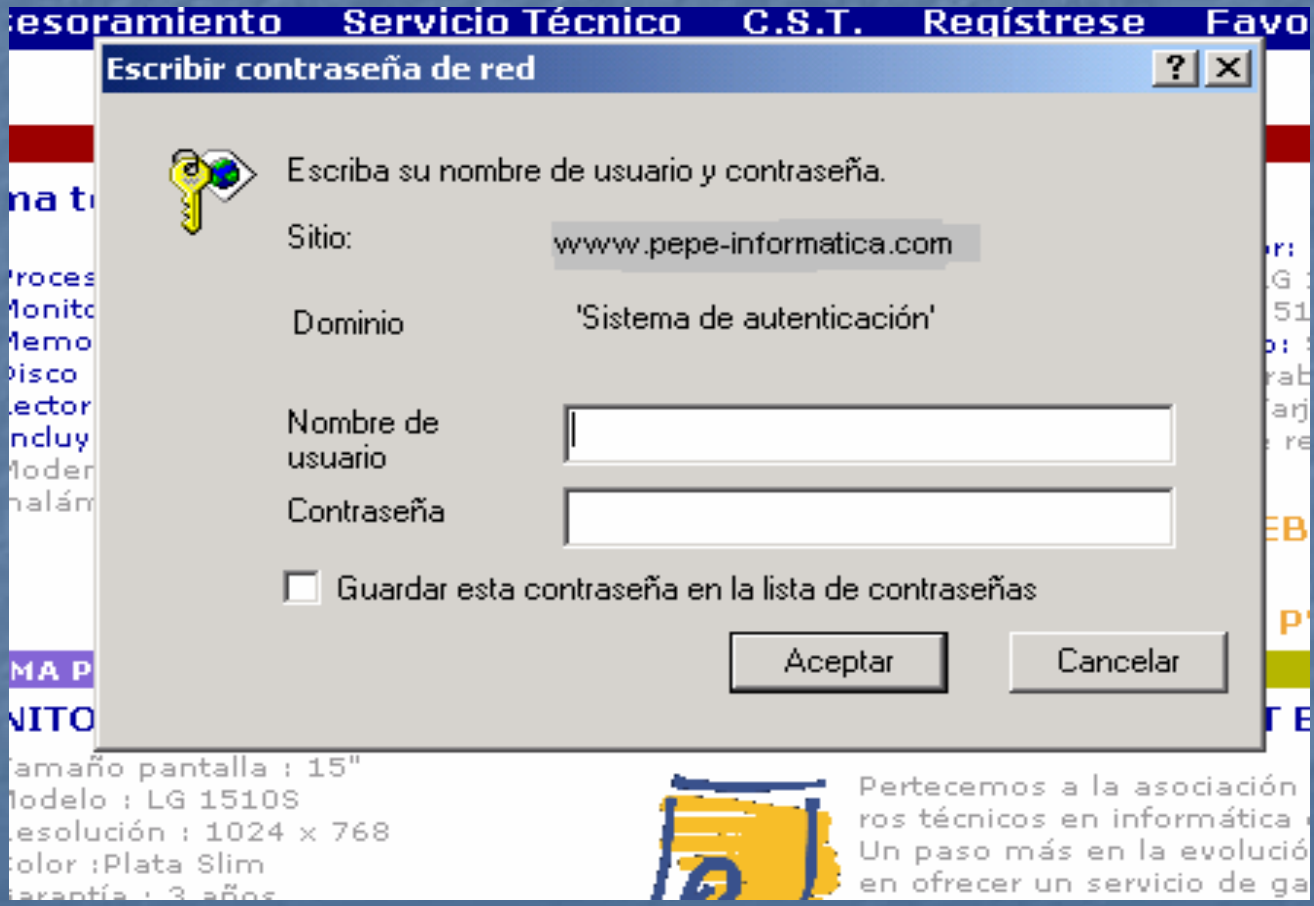
Control de acceso con PHP

```
$username = “tribilin”
$pwd = “secreta”
if (!isset($PHP_AUTH_USER)){
    Header(“WWW-Authenticate: Basic realm=\”Zona protegida\””);
    Header(“HTTP/1.0 401 Unauthorized”);
    Echo “Imposible ejecutar la autorizacion\n”;
    Exit
Else
    If (($PHP_AUTH_USER == $username) && ($PHP_AUTH_PW == %pwd)){
        Echo “Autorizacion ejecutada para $username”;
    Else
        Echo “$username no tiene autorización”;}
}
```

Control de acceso con PHP y mysql

```
<?function autentificar() {
header("WWW-Authenticate: Basic realm='Sistema de autenticación'");
header("HTTP/1.0 401 Acceso Denegado");
echo "<font 'verdana,arial' size='2' color='red'><center>Acceso denegado.\n </center></font>";
exit;
}
if(!isset($PHP_AUTH_USER)){ autentificar(); }
else {
 $link=mysql_connect("localhost", “localhost");
     mysql_select_db(“clientes",$link);
     $sql=sprintf("SELECT * FROM clientes WHERE nif='%s' AND clave='%s'",$PHP_AUTH_USER,$PHP_AUTH_PW);
     $sql=mysql_query($sql);
      if(mysql_num_rows($sql)==0){ autentificar(); }
     session_start();
     $usuario[0] = $PHP_AUTH_USER;
     $usuario[1] = $PHP_AUTH_PW;
     session_register(usuario);
}
?>
```

Apache - Seguridad



SSL – Secure Socket Layer

- Define canales seguros sobre TCP a servidores web. (pej. Envio de nº de tarjeta)
- Debe asegurar
  - Integridad
  - Confidencialidad
- Para instalar descargar el software :
  - www.apache.org (apache)
  - www.openssl.org (modssl)
  - www.modssl.org (modulo para apache)

SSL – Secure Socket Layer

- 2 formas de instalación :
  - 1.- Instalar por separado apache, modssl, y openssl (./configure && make && make install)
  - Crear el certificado
    - Openssl req –new > pepe-informatica.csr (Solicita datos y clave privada)
    - Openssl rsa –in privkey.pem –out pepe-informatica.key (Genera la clave que se añade al certificado)
    - Openssl x509 –in pepe-informatica.csr –out pepe-informatica.cert –req –signkey pepe-informatica.key –days 365. (Genera el certificado con un año de duracion)

SSL – Secure Socket Layer

- Modificar las directivas de apache.
  - AddModule mod_ssl.c
  - ...
  - LoadModule ssl_module modules/mod_ssl.so
  - ...
  - SSLLog logs/ssl.log
  - SSLLogleven warn
  - ...
  - <VirtualHost www.pepe-informatica.com:443>
    - SSLEngine on
    - SSLCertificateFile /ruta/pepe-informatica.cert
    - SSLCertificateKeyFile /ruta/pepe-informatica.key
    - ...
  - </VirtualHost>

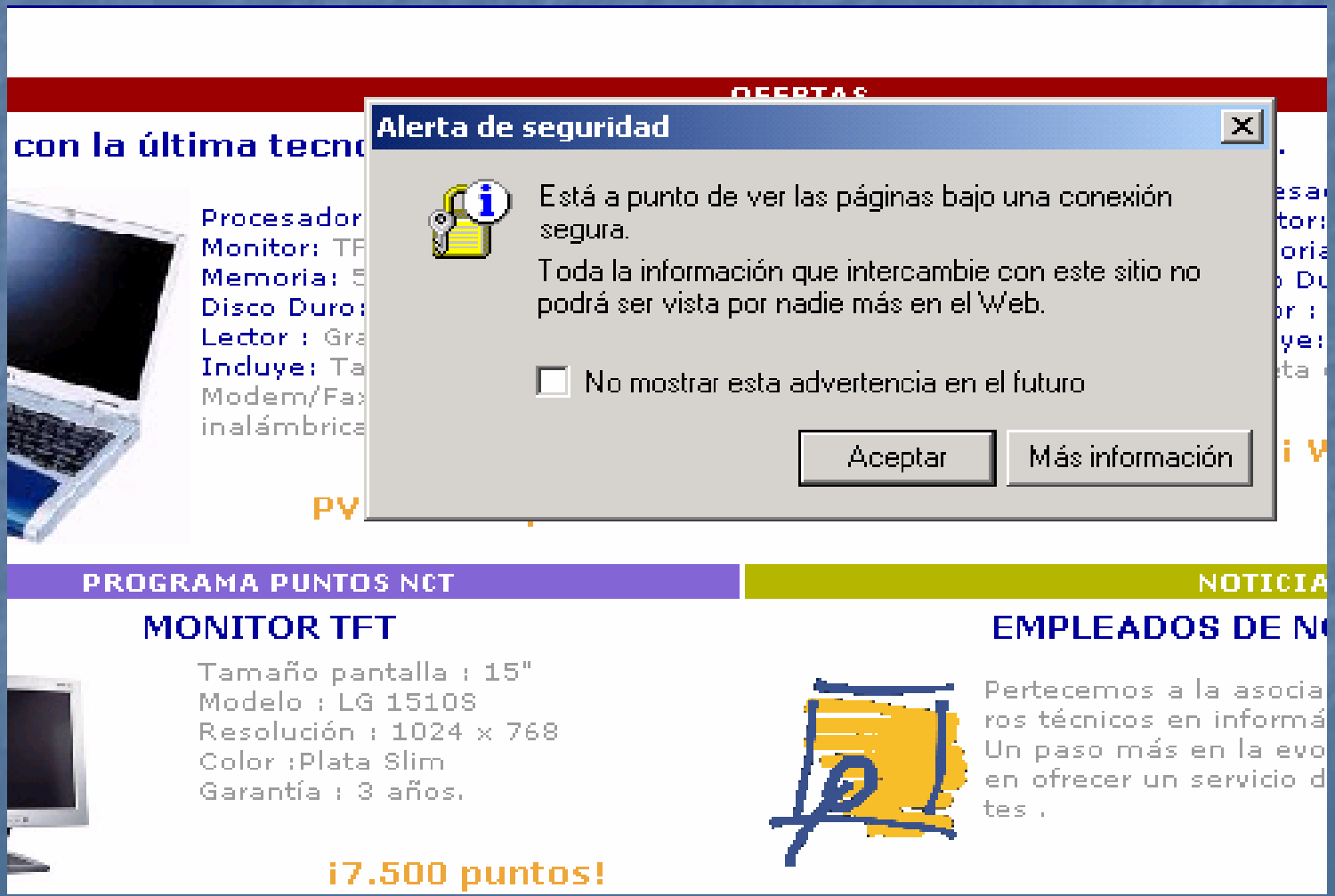
SSL – Secure Socket Layer

- Reiniciar apache. Puede que sea necesario usar el parámetro –D SSL o bien /usr/sbin/apachectl startssl
- Comprobacion
  - Openssl s_client –connect pepe-informatica.com:443
  - O bien httpS:\\www.pepe-informatica.com

SSL – Secure Socket Layer

- 2 forma de instalacion de Apache + SSL
  - Descomprimir e instalar openssl. Instalar con la configuración básica ./configure
  - Instalar openssl con la siguiente configuración
    - ./configure –with-apache=../rutaapche
  - Instalar apache con la siguiente configuración
    - SSL_BASE = ../rutaopenssl
    - ./configure –enable-module=ssl
    - Make
    - Make certificate (rellenar datos para el certificado)
  - Modificar las directivas de apache para que escuche para la dirección especificada.

SSL – Secure Socket Layer



SSL – Secure Socket Layer

Seguridad - FTP

- Aunque wu-ftp es la versión de la mayoria de las distribuciones no es la más usada.
- Tiene muchos agujeros de seguridad.
- Para solucionarlos es mejor crear una nueva aplicación.
- Otra solución es apostar por una aplicación distinta.

Seguridad - FTP

- PROFTPD nace por la necesidad de un servidor seguro de FTP.
- FTP servicio inseguro por naturaleza así que PROFTPD no es la panacea en seguridad.
- Servidor mas configurable y seguro.
- Permite entre otros...
  - FTP anónimo
  - Definir dominios virtuales
  - Control de permisos

Seguridad - FTP

- Si no es necesario es mejor deshabilitar este servicio y usar en su caso ssh sino tener en cuenta...
  - ¡Ojo! Las contraseñas viajan sin encriptar.
  - Probar si es posible escapar del directorio raíz.
  - Deshabilitar accesos anónimos en caso de pocos usuarios.
  - Evitar por encima de todo proporcionar permiso de escritura en los directorios.

Seguridad - FTP

- PRPFTPD al igual que Apache se configura mediante directivas. (muchas de ellas parecidas entre si)

- Crear usuario y grupo sin privilegios (proftpd) para que sea el encargado de ejecutar el servicio y no sea root el que lo haga.
  - User nobody o ftp
  - Group nogroup o ftp

Seguridad - FTP

- Allowoverride on/off : Para la sobreescritura de archivos.
- MaxClients nº “mensaje” : Limitarlos para evitar ataques DDoS.
- Port nº : Elegir el puerto por el que queramos escuchar.
- MaxInstances nº : Numero de conexiones ftp simultaneas. Limitar para evitar ataques Dos.
- Defaultroot ~ : Evitar que el usuario pueda ascender en el árbol de directorios.

Seguridad - FTP

- <Limit LOGIN> #controlar el acceso
  - Order deny, allow
  - Deny from competencia.com
  - Allow from all
- </Limit>
- Otras opciones para LIMIT en los directorios. READ, WRITE, STOR
- IgnoreHidden on/off : ocultar archivos.

Seguridad - FTP

- Archivos de logs.
- LogFormat nombre “formato”
  - Logformat default “%h %i %u %t”
- TransferLog /ruta/fich
  - TransferLog /Var/log/profptd/transfer
- ExtendedLog /ruta (AUTH|WRITE|READ|ALL) nombre.
  - ExtenderLog /var/log/proftpd.all.log ALL default.

Seguridad - SMTP

- SendMail servidor de correo de la mayoría de las distribuciones.
- Al igual que wu-ftp es inseguro.
- En su lugar se usan otros servidores de correo como postfix o qmail.
- Para instalarlos eliminar sendmail
  - Rpm –e sendmail nodeps

Seguridad - SMTP

- Ejecutar postfix con mínimos privilegios.
  - Default_privs = nobody
- Evitar el relay de correo salvo al nuestro para que no usen nuestra máquina para enviar SPAM.
  - Relay_domains = miequipo.com
- Limitar tanto el tamaño del buzón de correo como el tamaño de los correos en si.
  - Message_size_limit = 10485760
  - Mailbox_size_limit = 51200000
    - Para deshabilitar el limite se pueden poner a 0.

Seguridad - SMTP

- Notificaciones al postmaster
  - Bounce : si el mensaje no puede ser enrutado
  - 2bounce : si la notificacion de error tampoco puede ser enrutada.
  - Delay : mensajes con problemas de enrutamiento.
  - Policy: peticiones rechazadas de entregas de mensajes.
  - Software : el mensaje no se encamina por problemas de software.
    - Ej. Notify_classes = resource, software, policy

Seguridad - SMTP

- Filtrado de cabeceras:
  - Colocar en un fichero ej. Check_cabeceras
    /^Subject: Re: Your password!/
  - Header_checks = regexp:/ruta/check_cabeceras
- Filtrado de contenido:
  - Colocar en un fichero
    /Accept credit cards/ REJECTS
    /Nude Celebrities/ REJECTS
  - Body_checks = regexp:/ruta/check_body

FIN