Protocolo de seguridad

Existen numerosas configuraciones a la hora de montar un servidor para un Entorno Virtual de Aprendizaje. Lo que sigue es una guía, no exhaustiva, y propositiva con diversas tácticas que buscan economizar en tiempo y recursos, así como también prevenir posibles pérdidas de datos.

Contraseñas

Es importante aclarar que el tema de las contraseñas es crucial en lo que refiere a la informática. Las contraseñas de los estudiantes que se autentican por el sistema de bedelías (RADIUS), la gestionan ellos mismos por lo que no podemos hacer mucho al respecto. Pero para el caso de administradores, docentes, articuladores, etc., podemos ofrecer algunos consejos útiles desde el DATA.

Lo primero sería **utilizar contraseñas largas** (no menos de 6 caracteres) que **no puedan ser asociadas** con su nombre, ni usuario, y en general con ninguna otra información semi-pública. Por ejemplo el nombre de la institución al cual pertenece, el nombre de la calle de su casa, etc.

Preferentemente no utilizar palabras de diccionario y en lugar de esto, utilizar combinaciones de letras mayúsculas, minúsculas, símbolos y números. Sería muy útil inventar alguna regla mnemotécnica para poder recordar la contraseña. También es recomendable **no anotar la contraseña en un archivo de texto**, por lo que debe ser una contraseña fácil de recordar.

Finalmente y lo más importante de todo: **no enviar contraseñas por correo electrónico**. Si por algún motivo y alguna urgencia necesita enviar uno, hay herramientas con cierto nivel de seguridad que le permitirían hacerlo como: Privnote

Sistema Operativo

El punto de partida es tener un **sistema operativo seguro y robusto** en nuestro servidor, para poner en funcionamiento la serie de herramientas que permitirán la creación del Entorno Virtual de Aprendizaje. De ahora en más asumimos que usted trabajará con moodle como LMS (Gestor de contenidos de aprendizaje).

Debido a su seguridad, a su sistema de actualizaciones y a su gran comunidad y por supuesto por ser Software Libre, el DATA recomienda el uso de **GNU/Linux - Debian** (Web de Debian) como sistema operativo. Existe mucha documentación al respecto y tiene un buen equilibrio entre usabilidad y seguridad. En su defecto, puede elegirse también Ubuntu Server Edition. Recordemos que el 90% de las supercomputadoras utilizan sistemas basados en GNU/Linux, lo que aporta abundantes evidencias a considerarlo un sistema ideal para servidores: http://www.top500.org/stats/list/34/osfam

En cualquiera de los casos, es importante realizar las **actualizaciones** que el sistema sugiere. Tener un sistema sin actualizar por varias semanas o meses puede generar vulnerabilidades respecto a errores encontrados y corregidos por las comunidades que mantienen dichos sistemas.

Es importante a su vez estar atentos a la cantidad de usuarios que pueden acceder al sistema, así como también los servicios que se ejecutan en el mismo. La política **más restrictiva posible** es la mejor en estos casos. En el caso de Debian, nadie más que el administrador puede saber la contraseña del superusuario y en el caso de Ubuntu sería importante que solamente el administrador pertenezca al grupo adm que permite escalar a privilegios de superusuario ((En el caso de que el administrador desaparezca, siempre es posible, teniendo acceso físico al mismo, colocar un liveCD y hackear la password del superusuario)).

Asumimos también que usted instalará un servidor web y una base de datos (como MySQL o PostgreSQL) así como también php, ya que son los requisitos sobre los que trabajará moodle. Sobre esta serie de programas hay muchas recomendaciones posibles pero excede los alcances de este trabajo.

display_errors de php

Moodle nos avisa que debemos deshabilitar la directiva display_errors, como forma de evitar revelar información sensible del sistema. Por otro lado, el propio php nos advierte:

Even when display_errors is on, errors that occur during PHP's startup
sequence are not displayed. It's strongly recommended to keep
display_startup_errors off, except for when debugging.

En el caso de Ubuntu Server o Debian Lenny esta configuración está en /etc/php5/apache2/php.ini

Debe cambiarse la línea:

display_errors = On

por:

display_errors = Off

Finalmente reiniciar el servidor Apache:

sudo /etc/init.d/apache2 restart

Sincronización del reloj

Tanto por un tema de seguridad como de usabilidad, suele ser necesario sincronizar los relojes de los servidores, utilizando el protocolo NTP (http://es.wikipedia.org/wiki/Network_Time_Protocol). Esto evita la problemática de las diferencias en minutos del reloj del servidor con los de los usuarios.

La de-sincronización de relojes puede llevar a problemas a la hora de colocar los límites de entrega de trabajos, por ello el DATA recomienda utilizar herramientas como ntpd y ntpdate. En algún caso será necesario el ajuste de la configuración del Firewall.

Red

Para evitar posibles intromisiones en nuestro servidor, es necesario - además de restringir los servicios que corren - utilizar algún cortafuegos firewall . El data recomienda la utilización de NetFilter/iptables. En particular utilizar el software de generación de reglas Firewall Builder. FIXME: enlace

En este sentido, se recomienda abrir solamente los puertos 80 y el 443 para web, y en la medida de lo necesario algún puerto para administración remota. Al respecto es aconsejable utilizar openssh-server en un puerto diferente al 22 digamos x y abrir puerto x con las reglas mencionadas anteriormente (Donde x puede variar entre 1025 y 65535). Esto hace un poquito más dificultoso el escaneo de puertos y los intentos de hackeo.

Moodle

A nivel de Moodle el DATA recomienda la suscripción a sus avisos de seguridad y mantenerlo actualizado en la medida de lo posible. Pensamos que una **instalación manual** en este caso es lo recomendable ya que los repositorios Debian/Ubuntu no siempre tienen la versión más actualizada.

Si se instala manualmente hay que tener la precaución de desinstalar previamente la versión de los repositorios o de lo contrario bloquear la actualización. Una actualización automática (desde los repositorios) sobre una manual puede causar un problema importante.

Habría muchas recomendaciones al respecto, pero queremos hacer énfasis en la cantidad de usuarios con **roles definidos globalmente**. Aquí también la opción más restrictiva es la mejor. En este sentido, el DATA recomienda que haya un solo usuario con roles de administración global; en todo caso la administración de categorías y cursos puede realizarse otorgando privilegios de administración **a nivel de categoría**.

También aquí se hace necesario remarcar la cuestión de las contraseñas. La contraseña del administrador de moodle es otra de las cosas que debemos cuidar con mayor atención. Cuanto menos personas la conozcan mejor.

Por último, moodle presenta un resumen de los posibles riesgos de seguridad, accesible en el Menú Administración -> Informes -> Security Overview, o sino en la siguiente url: <url-de-eva>/admin/report/security/index.php

Recuperación de desastres

Este quizás sea uno de los temas centrales en cuanto al **manejo de información ajena y producida con mucho esfuerzo y dedicación** y de la cual la Universidad de la República es la última responsable. Refiere a realizar duplicados de la información, más conocidos como **respaldos**, de forma de poder recuperar la información de los usuarios en caso de problemas.

Los problemas pueden ser diversos: desde la rotura de un disco duro, hasta la posibilidad que se estropee una base de datos debido a un corte de luz o incluso un siniestro que deje inutilizable el servidor.

Existe una **multiplicidad de estrategias** al respecto, pero aquí solo presentaremos alguna que nos parecen las más adecuadas para nuestra universidad. Es así que supondremos que cada servicio tiene su servidor montado físicamente el edificio propio.

Si la computadora fue comprada específicamente para servidor, es muy probable que cuente con sistema de RAID por hardware -- esto es, dos discos duros que tienen en todo momento la misma información. Esto brindará la posibilidad de poner en funcionamiento al servidor casi inmediatamente en caso de rotura del disco duro.

De todos modos aun debemos solucionar dos cosas: **(i)** por un lado, la posibilidad de acceder a alguna copia pasada de nuestros datos y **(ii)** la posibilidad de un siniestro que deje disfuncional a ambos discos duros.

Se proponen 2 soluciones para atacar a los problemas (i) y (ii):

- La **solución óptima** es tener disponible un servidor de respaldos, preferentemente en un edificio distante al que se encuentra el EVA. En nuestro caso, tenemos esta configuración.
- La **solución mínima** sería comprar un disco duro externo con capacidad de 500MB o 1GB (por decir algo) para realizar los respaldos. En este caso sería conveniente llevar el disco duro con cierta periodicidad a otro edificio de la UdelaR y realizar una copia a otra pc (preferentemente almacenar los datos encriptados en la PC externa). Es necesario hacer énfasis en la importancia de resguardar la **privacidad y confidencialidad** de los datos.

En ambos casos, puede utilizarse el programa BackupPc para realizar las copias de seguridad. Este programa guarda mediante enlaces duros, copias de muchos días hacia atrás con un uso mínimo de espacio en disco. Por ejemplo, en el momento de escribir estas líneas el servidor EVA tiene un moodledata de unos 7,7GB y en el servidor de respaldos, hay hechos 5 respaldos completos y 8 incrementales, ocupando un total de 8,4GB en disco duro. Tenemos respaldos de 40, 26, 19, 12 y menos días de antigüedad; los de la última semana los tenemos todos. ¡Y solamente en 8,4GB!

FIXME: imagen de backuppc

De todos modos, es importante aclarar que existen otras alternativas libres como backup-manager, backula, etc. Hay una lista interesante de programas de respaldos aqui

Monitorización

La idea de este apartado es recomendar una forma de monitorear externamente nuestro servidor, y así acceder al estado general del sistema: uso de ram, de procesador, cantidad de procesos, tráfico de red, etc, etc.. Para ello es recomendable utilizar otra computadora ~~que puede ser la misma que usamos para respaldos~~ donde se instalará alguna de las alternativas libres para ello.

Existen varias posibilidades: FIXME:agregar enlaces

- zabbix
- cacti
- munin

Esta última es la recomendable, pues la hemos instalado y nos ha dado buenos resultados. Puede instalarse por los repositorios Debian/Ubuntu. Su página web es esta: http://www.zabbix.com

FIXME: imagen de zabbix.jpg

Desde el DATA podríamos llegar a acordar con cada servicio la posibilidad de utilizar el servidor de monitorización que tenemos configurado. Para ello se requeriría la apertura de 2 puertos y la instalación de un pequeño programa disponible en los repositorios Debian y Ubuntu.

Bibliografía

- **Chavez Flores, Alejandra.** *Informe de Seguridad Informática*. Octubre de 2009
- **OWASP** *Los diez riesgos más importantes en aplicaciones web*. http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project