Camuflando nuestro servidor Apache

Son muchos los peligros a los cuales un administrador puede verse enfrentado y mucho mas cuando se están ofreciendo servicios a todo el mundo y hay que permitir la entrada a nuestro sistema por un determinado sitio sin pedir autentificación. Los fallos que pueda haber en el software que se está utilizando y los parches que se hayan aplicado pueden determinar el daño que un usuario malintencionado llegue a hacernos.

Este manual no será de gran ayuda a un usuario normal de internet, ya que son pocos los que se ven en la obligación de instalar y poner en marcha un servidor web como Apache, pero si será de alguna utilidad a quién desee ver aspectos básicos de la seguridad informática y sobre todo a aquellos que disfruten sin mas del hecho de aprender. Descargaremos el código fuente de su página web, lo modificaremos, compilaremos y veremos los resultados obtenidos ante un posible ataque al mismo.

Bien, supongamos que hemos instalado y configurado nuestro servidor web y que está corriendo sin ningún problema, pero resulta que un usuario malintencionado ha detectado nuestro web server con un escaneo de puertos y ahora quiere identificar que versión de Apache tenemos instalada, para posteriormente buscar bugs en esa versión y utilizar el correspondiente exploit contra nuestro sistema. Veamos como averiguaría dicho dato (utilizaremos la dirección 127.0.0.1 como dirección del sistema víctima):

vlad@saruman:~$ telnet 127.0.0.1 80

Trying 127.0.0.1...

Connected to 127.0.0.1.

Escape character is '^]'.

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Sat, 30 Sep 2006 08:48:57 GMT

Server: Apache/1.3.37 (Unix)

Content-Location: index.html.en

Vary: negotiate,accept-language,accept-charset

TCN: choice

Last-Modified: Thu, 06 Jan 2005 12:11:39 GMT

ETag: "11185-5b0-41dd2afb;451e2f2d"

Accept-Ranges: bytes

Content-Length: 1456

Connection: close

Content-Type: text/html

Content-Language: en

Expires: Sat, 30 Sep 2006 08:48:57 GMT

Connection closed by foreign host.

Lo que ha hecho es conectarse al puerto 80 de nuestro sever y una vez allí lanzar la petición **HEAD / HTTP/1.0** seguida de dos intros para que le apareciese en la terminal toda esa información. Si el sistema víctima no hubiera aceptado esa petición, podría haber intentado **GET / HTTP/1.0/** . En dicha información, aparece la siguiente linea:

Server: Apache/1.3.37 (Unix)

Nuestro atacante ya sabe que se trata de la versión 1.3.37 de Apache y que además el host es de tipo Unix y esto lo que queremos evitar, así que pongamonos manos a la obra.

Lo primero que vamos a hacer es descargarnos el código fuente de http://apache.rediris.es/httpd/, una vez en nuestro poder lo descomprimimos y editamos el archivo *http.h* que está situado en el directorio *apache_1.3.37/src/include/* y buscamos las lineas:

#define SERVER_BASEPRODUCT "Apache"

#define SERVER_BASEREVISION "1.3.37"

Las podemos cambiar por lo siguiente:

#define SERVER_BASEPRODUCT "Sin información"

#define SERVER_BASEREVISION "Sin información"

Guardamos el archivo y editamos también *apache_1.3.37/src/main/http.main.c,* buscamos las lineas:

```
else {
    ap_add_version_component(SERVER_BASEVERSION " (" PLATFORM ")");
```

Y las dejamos en:

```
else {
```

ap_add_version_component(SERVER_BASEVERSION);

Luego volvemos a compilar desde el directorio principal con:

./configure

make

su

make install

Arrancamos el servidor y vemos cual sería el resultado del ataque en busca de información hacia nuestro servidor:

vlad@saruman:~$ telnet 127.0.0.1 80

Trying 127.0.0.1...

Connected to 127.0.0.1.

Escape character is '^]'.

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Sat, 30 Sep 2006 10:09:20 GMT

Server: Sin información/Sin información

Content-Location: index.html.en

Vary: negotiate,accept-language,accept-charset

TCN: choice

Last-Modified: Thu, 06 Jan 2005 12:11:39 GMT

ETag: "11185-5b0-41dd2afb;451e2f2d"

Accept-Ranges: bytes

Content-Length: 1456

Connection: close

Content-Type: text/html

Content-Language: en

Expires: Sat, 30 Sep 2006 10:09:20 GMT

Connection closed by foreign host.

Como podemos ver, ya no existe información disponible sobre el servidor web que es ni la versión del mismo, así como del tipo de plataforma del que se trata. Objetivo cumplido. He aquí un claro ejemplo de lo que supone el movimiento OpenSource, la disponibilidad del código fuente de una aplicación es una gran ventaja para el administrador, que puede modificarlo según sean sus circunstancias o intereses.

Año 2006.

Por Vl@d.

Para www.fentlinux.com