Ejercicios de Seguridad: Taller CEDIA

3 de Marzo, 2004

1.) Apagamos servicios no necesarios

Como vamos a hacer esto?

Como buscamos que esta corriendo?

Como root, o usando "sudo":

```
lsof -i
netstat -natup
cd /etc/rc.d/init.d/
chkconfig --list | more
```

Que quiere correr y no correr? Elige, y apaga servicios que no quiere correr. Como va a apagarlos?

Una pista...

```
chkconfig...
```

2.) Protegemos un servicio using tcpwrapper (xinetd)

Vamos a inicializar un servicio medio seguro, y tratamos de hacerlo mas seguro por nuestro ambiente.

Vamos a inicializar el servicio FTP usando el tcpwrapper xinetd.

Primero, antes de inicializar FTP configuramos el program para ser un poco mas seguro. Abre el archive /etc/vsftpd.conf (como root o usando sudo). Busca las lineas mostradas y cambiarlas como muestro abajo:

```
anonymous_enable=YES
local_enable=NO
write_enable=NO
ftpd_banner=Bienvenido a mi servidor FTP
tcp_wrappers=YES
```

Ahora graba el archivo (:wq)

Trata de abrir el archivo /etc/xinetd.d/ftp (como root o usando sudo). Que harias si no existe este archivo? Usa cp otro_archivo ftp y cambia los campos apropiados...

Ahora, queremos que el archivo de ftp se vea asi:

```
# default: on
# description: The ftp server serves ftp sessions; it uses \
#       unencrypted username/password pairs for authentication.
service ftp
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/vsftpd
        only_from       = 192.188.58.0
        no_access       = 192.188.58.xx
        log_on_failure  += USERID
        disable         = no
}
```

En el campo "no_access" por la direccion (vea el "xx") pon la direccion de PC vecino a ti. Por ejemplo, si tu direccion es 192.188.58.69 y tu vecino es 192.188.58.70, entonces pon 192.188.58.70 en el campo "no_access".

Si tienes preguntas sobre los campos en este archvio lea:

```
man xinetd.conf
```

Ahora vamos a prender el servicio de FTP (Red Hat usa VSFTP, o "Very Secure FTP"). Como inicializaria el servicio FTP en este caso?

Una pista...

```
cd /etc/rc.d/init.d
```

Y, ahora tiene que reinicialzar...?

```
./xinetd restart
```

Ahora, probamos si FTP esta funcionando:

```
ftp localhost
```

Trata de entra como un usuario en tu sistema. Deberia fallar. Pero, trata como "anonymous" y "nombre@maquina" - deberia funcionar.

Finalmente, trata de conectar al FTP a la maquina vecina tuya que tiene en su configuracion de /etc/xinetd.d/ftp la direccion IP du tu maquina en el campo "no_access.

3.) Aplicar una actualizacion de software

Red Hat sale con actualizaciones de software por su distribucion. Hemos copiado las mas recientes al servidor aca. Conectarse al servidor de clase (noc en /etc/hosts o 192.188.58.125) y vea la lista de actualizaciones que hay:

```
ftp noc (192.188.58.126)
anonymous
usuario@direccion
cd pub/redhat9/updates/i386
ls http*
ls mod*
ls open*
```

Notaste que hay varias actualiaciones que paren importante. Hay mucho mas, pero vamos a parchar Apache, y el subistema de SSL por Apache, y OpenSSL en este momento.

Para hacer esto vamos a bajor los archivos que necesitamos a /usr/local/src in nuestras maquinas. No vamos a parchar el kernel en este momento.

Este es un paso a la seguridad. Por ejemplo, si usted esta corriendo o usando SSH y si hay un ojo de seguridad en SSH deberias parchar tu servidor y clientes luego. Entonces, para hacer esto haz lo siguiente (conectado al noc con FTP todavia):

```
lcd /usr/local/src
binary
mget openss*
[responde no a los paquetes openssl096b - hay dos]
mget mod_ssl*
mget httpd-*
exit
```

Ya tienes los paquetes de RPM que van a hacer una actualizacion a los servicios de http y ssh en tu maquina y al codigo de encifricazion ssl.

Antes de instalar los paquetes piensa en que significa. Hay servicios corriendo que tienes que apagar? Que se puede quebrar?

Ahora instal los paquetes en este orden. Esto es *importante* que sigues el order. RPM no resuelve las dependencias entre paquetes. Vas a encontrar dos problemas con esto. Pregunta a los ayudantes por ayuda. Entonces, instala los paquetes asi:

openssl-0.9.7a-20
openssl-devel-0.9.7a-20
openssl-perl-0.9.7a-20

openssh-3.5p1-11
openssh-askpass-3.5p1-11
openssh-askpass-gnome-3.5p1-11
openssh-clients-3.5p1-11

[Antes de actualizar el servidor de ssh que tienes que hacer? Para el servicio sshd.]

Ahora instala asi:

openssh-server-3.5p1-11

Si se instalo que haces? [inicializar el servicio de nuevo.]

Ahora hacemos actualizaciones al servidor de web y a su sistema de seguridad ssl que corre con el servidor:

Primero tiene que parar el servicio de httpd.

Ahora instala en este orden:

httpd-2.0.40-21.9
[nota /etc/httpd/conf/httpd.conf como httpd.conf.rpmnew!]
httpd-devel-2.0.40.21.9
httpd-manual-2.0.40.21.9

Y, finalmente:

mod_ssl-2.0.40-21.9

Notaste como se sigue la misma version entre paquetes relacionados? Ahora inicializa de nueve el servicio httpd.

Pruebe que las cosas sigue funcionando.

ssh a una maquina.

lynx https://localhost/

4.) Instalar libsafe encontra ataques de Buffer Overflow

Libsafe es una solucion encontra los ataques de buffer overlow que usa un nivel de software que intercepta todo las llamadas de funciones a funciones de bibliotecas que tienen oyos de seguridad. Los funciones incluyen:

```
strcpy(char *dest, const char *src)
strpcpy(char *dest, const char *src)
wcscpy(wchar_t *dest, const wchar_t *src)
wcpcpy(wchar_t *dest, const wchar_t *src)
       May overflow the dest buffer.

strcat(char *dest, const char *src)
wcscat(wchar_t *dest, const wchar_t *src)
       May overflow the dest buffer.

getwd(char *buf)
       May overflow the buf buffer.

gets(char *s)
       May overflow the s buffer.

[vf]scanf(const char *format, ...)
       May overflow its arguments.

realpath(char *path, char resolved_path[])
       May overflow the path buffer.

[v]sprintf(char *str, const char *format, ...)
       May overflow the str buffer.
       May exploit "%n".
```

Entonces, si uno instala libsafe y alguin trata de entra tu sistema usando un buffer overflow durante una llamada a una de estas funciones, libsafe protege tu maquina encontra esto. Por ser caso, esto es uno de los oyos de seguridad que esta explotada mas en el mundo de Linux.

Para conseguir el software de libsafe conectarse al noc usando ftp. Deberia ser root cuando haces esto:

```
ftp noc (192.188.58.126)
anonymous
usuario@direccion
cd pub/software/libsafe
binary
lcd /usr/local/src
mget *
exit
```

Ahora vamos a hacer un chequeo del archivo de libsafe. Vaya a /usr/local/src. Nota que hay un archivo que se llama "md5". Esto tiene la firma del archivo libsafe-2.0-16.tgz. Say genera este firma haciendo "md5sum archivo > firma.txt". La idea es que este algoritmo genera una firma unica por el archivo (nunca han visto dos firmas de md5 iguales en el mundo).

Usando esto si la firma que generas tu, y la firma que bajas son iguales, asi puedes verificar que nadie he tocado el archivo. Si uno cambia un bit en el archivo la firma va a cambiar - y se cambia mucho.

Entonces, haz:

```
cd /usr/local/src
md5sum libsafe-2.0-16.tgz > firma.txt
diff firma.txt md5
```

Si no veas una respuesta del comando diff (diferencia) significa que los archivos son iguales. Mira adentro firmat.txt y md5 (cat firma.txt, etc.).

Ahora vamos a descomprimir y expander el archivo libsafe-2.0-16. Recuerdas como hacer esto?

```
tar xvzf libsafe-2.0-16.tgz
cd libsafe-2.0-16
```

Ahora, tenemos decisiones para hacer. Siempre antes de instalar algo deberias leer la documentation. En este caso los archivo INSTALL y README. Entonces:

```
less README
less INSTALL
```

Si leiste ambos vas a contar que hay una opcion para instalar libsafe en una maner para que si hay un ataque de buffer overlow a tu maquina un correo esta mandado a root@localhost o a los usuarios en el archivo /etc/libsafe.notify si existe el archivo. Para que libsafe hace esto tienes que cambiar las opciones de compilacion en el archivo src/Makefile. Vamos a hacer este Cambio.

Abre el archivo src/Makefile asi, "vi src/Makefile".

Vaya a la linea 77 (:77)

Cambia la linea que lea:

```
CCFLAGS         = -O2 -Wall -fPIC -DLIBSAFE_VERSION=\"$(VERSION)\" $(LIBPRELUDE_CFLAGS)
```

para que se dice:

```
CCFLAGS         = -O2 -Wall -fPIC -DNOTIFY_WITH_EMAIL -DLIBSAFE_VERSION=\"$(VERSION)\" $(LIBPRELUDE_CFLAGS)
```

Y, ahora para instalar libsafe:

```
make
make install
```

Y, ahora lea los mensajes y "man libsafe" - Tienes que especificar al sistema que va a usar libsafe. Puede hacer esto temporariamente y permanente (poniendo el variable nuevo de ambiente en /etc/profile). Pero, para correr libsafe ahora mismo, cambia tu shell asi:

LD_PRELOAD=/lib/libsafe.so.2
export LD_PRELOAD

Y, ya estas usando libsafe.

Para leer mas sobre libsafe vaya a:

http://www.research.avayalabs.com/project/libsafe/

Hervey Allen
Marzo 2004

Last modified: Tue Mar 2 13:39:54 ECT 2004