3. CAPÍTULO TRES - DESARROLLO DE SERVIDOR WHOIS PARA PROVEER INFORMACIÓN DE CONTACTO DE ADMINISTRADORES DE RED-UNAM

En este capítulo explico el objetivo, marco teórico, desarrollo, instalación y configuración del servidor whois utilizado para proveer información de contacto de administradores de redes de datos de RED-UNAM, así como una descripción de los programas adicionales que desarrollé para instalarlo y administrarlo.

3.1. Antecedentes

De acuerdo a la Guía de Manejo de Incidentes de Cómputo del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST 800-61 – CSRC), uno de los puntos más importantes en la respuesta a incidentes es la rápida notificación de éstos:

"When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals within the organization and, occasionally, other organizations.

Timely reporting and notification enable all those who need to be involved to play their roles."

Traducción al español:

"Cuando un incidente es analizado y se le asigna una prioridad, el equipo de respuesta a incidentes necesita notificarlo a las personas responsables dentro de la organización y ocasionalmente a otras organizaciones.

Una notificación oportuna permite que todas las personas involucradas desempeñen su papel de manera adecuada. "

Es una tarea fundamental de los equipos de respuesta a incidentes de seguridad contar con los medios para reducir los tiempos de notificación para dar una solución más rápida a los incidentes de seguridad.

3.2. Objetivo

Instalar, configurar, administrar y documentar un servidor whois que permitió acceder de una manera rápida y fácil a miembros de respuesta de incidentes de UNAM-CERT y a miembros de Departamento de Redes de la DGTIC a la información de la base de datos de administradores de RED-UNAM, con el fin de que el tiempo de notificación de los incidentes de seguridad fuera mínimo y los incidentes de seguridad se resolvieran más rápido.

3.3. Marco teórico

La red de datos utilizada por dispositivos pertenecientes a la UNAM es conocida como RED-UNAM. Por su tamaño es un sistema autónomo, tiene asignado el número 278, dos segmentos completos clase B (132.248.0.0/16 y 132.247.0.0/16) y está registrada con el nombre Red Académica de México, como se puede apreciar en la figura 3.1

```
david@david-desktop:~$ whois -h whois.cymru.com -v 132.248.1.1
Aviso: Los indicadores RIPE son ignorados por los servidores tradicionales.
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
278     | 132.248.1.1      | 132.248.1.0/24      | MX | lacnic   | 1989-03-31 | Red Academica de Mexico
david@david-desktop:~$ whois -h whois.cymru.com -v 132.247.1.1
Aviso: Los indicadores RIPE son ignorados por los servidores tradicionales.
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
278     | 132.247.1.1      | 132.247.0.0/16      | MX | lacnic   | 1989-03-31 | Red Academica de Mexico
```

Fig. 3.1 Información de Sistema Autónomo de RED-UNAM.

El número total de direcciones IP utilizables para un segmento clase B es 2^16 -2 = 65,534

Por lo tanto, el número máximo de direcciones disponibles de RED-UNAM considerando los dos segmentos es de aproximadamente 131,068. Debido al uso de subredes y VLSM en RED-UNAM, las direcciones IP utilizables son menos, debido a que algunas direcciones IP son ocupadas como direcciones de segmento de red y direcciones de broadcast. Esta cifra basta para mostrar el gran tamaño de RED-UNAM y la amplia cantidad de dependencias que tiene y, como consecuencia, la dificultad que supone su administración.

Para la notificación de RED-UNAM el UNAM-CERT cuenta con un Sistema de Atención a Incidentes (SAI) que tiene una base de datos de los administradores de los distintos segmentos de asignados a varias dependencias de RED-UNAM. Este sistema permitió, antes de la realización del sistema whois, que personal de respuesta a incidentes de seguridad se pusiera en contacto con los administradores de las diferentes redes de RED-UNAM para notificar incidentes, sin embargo tiene las siguientes limitaciones:

- No permite que personal externo a UNAM-CERT, en particular personal del Departamento de Redes de la DGTIC, tenga la posibilidad de consultar la información de los administradores de RED-UNAM.
- El uso del Sistema de Atención a Incidentes sólo es accesible desde la red local, además de que requiere un proceso de autenticación
- No permite que la información de los administradores pueda ser utilizada mediante programas externos desde línea de comandos, únicamente desde el SAI.

También realicé un manual para la instalación y configuración de la aplicación swhoisd, que fue en la que se basó el sistema además de modificar el código fuente para ajustarlo a las necesidades particulares de UNAM-CERT.

El servidor whois permitió que esta información no fuera exclusiva de UNAM-CERT sino que pudiera ser compartida con personal del Departamento de Redes de la DGTIC, con el fin de que ellos también pudieran contactar a los administradores responsables de redes de la UNAM para solucionar rápidamente problemas de redes y conectividad. La mejor manera de alcanzar los objetivos planteados en el proyecto fue por medio de la implementación de un servidor whois.

3.4. Servicio Whois

Este servicio está definido en varios documentos de Solicitud de Comentarios RFC [1]. El más reciente de ellos es el RFC3912 [2]. el cual es una versión actualizada del documento RFC 954 [3], el cual a su vez es una versión actualizada del RFC 834 [4]

El servicio whois utiliza usa el puerto TCP 43 y el modelo cliente/servidor. El RFC 3912 indica lo siguiente:

"WHOIS es un protocolo cliente-servidor orientado a conexión que utiliza el protocolo de transporte TCP y es usado ampliamente para proveer servicios de información a usuarios de internet. A pesar de que originalmente fue usado para proveer servicios de información sobre nombres de dominio y segmentos de red registrados, desarrollos actuales se utilizan para cubrir un amplio rango de servicios de información. El protocolo entrega su contenido en un formato que puede entender una persona."

El RFC 834 indica lo siguiente:

"Un servidor básicamente recibe una dirección IP y responde con un conjunto de datos asociados a la misma. Como lo define el RFC, este servicio se basa en una transacción TCP bajo la arquitectura cliente/servidor que corren en algunas computadoras centrales que proveen servicio de directorios globales disponible para los usuarios de Internet. El Centro de Información de la Red (NIC) provee el servidor central de base de datos para los nombres de NIC, como se definen en el RFC 954 y permiten realizar búsqueda de individuos, organizaciones de red, nombres de equipos y más información de interés para los usuarios de internet. "

La organización encargada de proveer los números y nombres de Internet ICANN (antes IANA) tiene a su vez las siguientes oficinas locales (RIRs) ubicadas en varias regiones del mundo:

AfriNIC: Región Africana
APNIC: Región Asía y Pacífico
ARIN: Región de Canadá, Estados Unidos y algunas islas del Atlántico Norte y del Caribe
LACNIC: Región de Latino América y el Caribe
Ripe: Europa, partes de Asia y Medio Oriente [5]

Cada uno de los RIRs administra sus propios servidores whois, que utilizan para difundir la información de las organizaciones que tienen registradas determinadas direcciones de Internet, el cual es el uso más común que se le da a los servidores whois. De la misma manera y en menor medida, hay algunas organizaciones como la UNAM, que proveen la información de sus redes mediante este servicio a usuarios dentro de la misma organización.

3.5. Instalación

El servidor en el que se instaló cuenta con un sistema operativo GNU/LINUX Debian versión 5 (Lenny) con kernel 2.6.26-2-686

3.5.1. Requisitos

Antes de instalar el servidor whois, es necesario instalar los paquetes que éste requiere para su funcionamiento, los cuales se describen en la tabla 3.1

Programa	Propósito	Comando(s) de instalación
Build-essential	Compilador de c y otras herramientas de desarrollo de aplicaciones.	`apt-get install build-essential`
CVS	Gestión de versiones de software	`apt-get install rcs`
Autoconf	Programa para desarrollo de aplicaciones	`apt-get install autoconf`
Gettext	Programa para traducción de mensajes.	`apt-get install gettext`

Automake	Programa de desarrollo de aplicaciones.	`wget http://ftp.gnu.org/gnu/automake/automake-1.6.3.tar.gz`
		`tar –xzf automake-1.6.3.tar.gz`
		`cd automake-1.6.3`
		`./configure && make && make install`

Tabla 3.1 Requisitos del servidor swhoisd

Una vez instalados los programas requeridos, se descarga el código fuente del servidor swhoisd, se descomprime y se accede al directorio `swhoisd-3.0.5`.

```
wget ftp://dan.drydog.com/pub/swhoisd/swhoisd-3.0.5.tar.gz
tar –xzf swhoisd-3.0.5.tar.gz
cd swhoisd-3.0.5
```

Antes de instalar el servidor, es necesario realizar algunas modificaciones en los archivos del sistema, con el fin de optimizar la aplicación.

3.5.2. Modificación del código fuente

Para incrementar la velocidad de respuesta del servidor, modifiqué el código del archivo main.c, para asignar a cero la variable de retardo:

```
#define DEFAULT_DELAY_TIME 0 /* seconds */
```

Modifiqué los siguientes archivos para reemplazar las palabras en inglés por palabras en español y personalizadas para el UNAM CERT.

Realicé modificaciones en el archivo `src/do_whois.c`, programa responsable de implementar la lógica del servidor y la impresión de mensajes.

Nota: El uso de acentos afecta el uso de la aplicación, ya que por ser ASCII estándar funciona con el código ASCII, el cual no reconoce acentos.

Se realizaron principalmente reemplazos en los mensajes en inglés por mensajes en español personalizados para UNAM-CERT en el archivo `src/do_whois.c`, así como cambios en la lógica del programa para ajustarlo a la funcionalidad deseada, para permitir realizar búsquedas por dirección IP y mostrar los segmentos de red asignados a cada Dependencia.

3.5.3. Compilar e instalar la aplicación

Desde el directorio swhoisd-3.0.5, ejecutar el siguiente comando:

```
./configure && make && make install
```

Si la instalación se ejecuta correctamente, al final se mostrará el mensaje

```
make[1]: se sale del directorio ´/usr/src/swhoisd-3.0.5´
```

3.6. Configuración

El servicio de whois es ejecutado por el demonio in.swhoisd. Éste puede ser ejecutado directamente o por medio del servidor inetd (servidor de servidores).

3.6.1. Configuración mediante inetd

Cuando inetd recibe una conexión, se determina qué servicio debería responder a la misma, se lanza un proceso que ejecuta dicho servicio. La ejecución de una única instancia de inetd reduce la carga del sistema en comparación con lo que significaría ejecutar cada uno de los servicios que gestiona de forma individual.

Agregar la siguiente línea al archivo /etc/inetd.conf,

```
whois stream tcp nowait root /usr/sbin/in.swhoisd in.swhoisd
```

Reiniciar el súper servidor inetd:

```
#/etc/init.d/openbsd-inetd restart
```

Confirmar que se da de alta el servicio con el comando:

```
# netstat –atpn
```

Buscar un servicio non nombre inetd escuchando en el puerto 43.

3.6.2. Configuración como aplicación independiente

Una de las maneras de ejecutar el servidor whois es como aplicación independiente, lo cual permite que la respuesta del servicio sea más rápida, debido a que las peticiones no necesitan pasar primero por el proceso de inetd. Para poner a la escucha el servidor whois como aplicación independiente, basta ejecutar el comando:

```
#/sbin/in.swhoisd
```

3.6.3. Configuración de la base de datos

La base de datos de Administradores del SAI debe de colocarse en el archivo `/etc/swhoisd.conf`, que es de donde el servidor whois buscará el patrón a buscar y proporcionará la información correspondiente.

Modifiqué el código fuente de la aplicación para que se ajustara a los campos deseados. Por ejemplo, los datos de una IP que pertenece al UNAM-CERT se mostrarán de la siguiente forma:

```
Depe23 nr {
 !address 132.248.124.133
 !name  DGTIC, SSI/UNAM-CERT
 contact (1) Rubén Aquino Luna, Subdirector de Seguridad de la Información
 phone  56228169
 email  raquino@seguridad.unam.mx
 contact (2) Roberto Sánchez Soledad, Responsable del Área de Atención a
Incidentes
 phone  56228169
 email  rsanchez@seguridad.unam.mx
 red 132.248.124.0,124-192
```

3.7. Administración

Para controlar el demonio `in.swhoisd` se provee, en la aplicación original, un script de bash para iniciarlo, detenerlo y reiniciarlo. Este script está diseñado para distribuciones basadas en Red-Hat, por lo que realicé el siguiente script para la distribución LINUX Debian. Le incorporé las siguientes mejores que no fueron consideradas en el script de Red Hat:

- Validación de privilegios.
- Validación de estado (si se intenta iniciar y el servicio ya está iniciado, imprime el mensaje de error correspondiente y lo mismo ocurre cuando está detenido).
- Obtención de status. Permite observar si está detenido y si está escuchando y en qué puerto, así como el identificador de proceso del servidor.
- El funcionamiento del script se puede auditar, ya que guarda un registro en la bitácora del sistema `/var/log/messages` cada vez que inicia o termina junto con la fecha y hora del evento.

3.7.1. Código fuente del script de administración swhoisd

```
#! /bin/sh

# 4 de agosto de 2010 - David Bernal
# Descripción: Este servicio permite a los usuarios obtener información de la
Base de Datos del SAI mediante un cliente whois estándar.
# Nombre del proceso: in.swhoisd

if [ ! "$EUID" -eq 0 ];then
  echo "Se requieren privilegios de súper usuario."
  exit 1
fi
start() {
  echo -n $"Iniciando el servidor whois:  "
  if [ ! -z "$(netstat -atpn | grep in.swhoisd)" ];then
    echo "El servicio ya está activo. Ejecute restart para reiniciarlo."
    exit 0
```

```
  else
    in.swhoisd
    RETVAL=$?
    [ $RETVAL -eq 0 ] && echo "Servidor iniciado" &&  echo $(date)"  Servidor
whois iniciado" >> /var/log/messages
     return $RETVAL
  fi
}

stop() {
  echo -n $"Deteniendo servidor whois: "
  if [ -z "$(netstat -atpn | grep in.swhoisd)" ];then
    echo "Servicio no iniciado"
    exit 0
  else
     killall in.swhoisd
     RETVAL=$?
     [ $RETVAL -eq 0 ] && echo "Servidor whois detenido" &&  echo $(date)"
Servidor whois detenido" >> /var/log/messages
     return $RETVAL
  fi
}

restart() {
  stop
  start
}

# Selecciona la acción a ejecutar
if [ "$#" -eq 0 ];then
  start
  exit 0
fi

case "$1" in
start)
start
       ;;
stop)
stop
       ;;
status)
stat=$(netstat -atpn | grep in.swhoisd)
if [ -z "$stat" ];then
  echo "Servicio whois no iniciado"
  else
  echo "$stat"
fi
       ;;
restart)
restart
       ;;
 *)
echo $"Uso: $0 {start|stop|status|restart}"
exit 1
       ;;
esac
exit $?
```

3.7.2. Manejo del servidor mediante el script de administración swhoisd

La administración del servidor `swhoisd` se realiza por medio del script `/etc/init.d/swhoisd` como se indica en la tabla 3.2.

Acción	*Opción*	*Comando*
Iniciar	start	`# /etc/init.d/swhoisd start`
Detener	stop	`# /etc/init.d/swhoisd stop`
Reiniciar	restart	`# /etc/init.d/swhoisd restart`
Revisar el estado	status	`# /etc/init.d/swhoisd status`

Tabla 3.2 Descripción de las opciones del script de administración swhoisd

3.7.3. Configuración de inicio.

Para iniciar el servidor cada vez que se carga el sistema operativo, se agregó un servicio con prioridad 80 para cargar el servidor whois al inicio del sistema.

```
# ln -s /etc/init.d/swhoisd /etc/rcS.d/S80whois
```

3.7.4. Programa para instalación automática

Desarrollé un script instalador en lenguaje en bash shell que permitió instalar el servidor whois y sus dependencias, así como los scripts de administración y actualización fácilmente, el cual además facilitaría su migración a otro servidor en caso de ser necesario.

Además configura el archivo de manejo del servidor `/etc/init.d/swhoisd` que expliqué en la sección anterior e instala una versión de prueba de la base de datos del sistema SAI. También contiene documentación y muestra mensajes al usuario indicando si se instaló correctamente o si se registró algún error, por lo que su funcionamiento es más claro que la aplicación original.

Después de instalar el servidor whois, ejecuta el script `whois.pl` para crear una base de datos de prueba y así verificar la correcta funcionalidad del servidor.

Finalmente, agrega una liga suave en el directorio `/etc/rcS.d` para que el servicio se instale cada vez que se inicie el sistema. Al finalizar imprime un mensaje indicando que se lea el archivo de documentación `LEEME.txt`.

Esto permitió optimizar y facilitar la instalación del servicio whois en el servidor de producción y permitirá que sea fácil de instalar en otros servidores en caso de ser necesario. Además en el auto instalador corregí los problemas originales de la herramienta swhoisd, ya que tiene un archivo de verificación de requerimientos (configure) que no detecta correctamente los requisitos de instalación y causa que falle la instalación del servidor al ejecutar la sentencia make.

A continuación se incluye el código fuente del script instalador del servidor whois.

```
#!/bin/bash
# David Bernal Michelena
# Script de instalación del servidor whois

ruta="$(pwd)"
whois="swhoisd-3.0.5"
parser=ParserSAI

`which make > /dev/null`
if [  $? -eq 0 ] ;then
        echo " make instalado"
else
        echo "Instalando build-essential"
        apt-get install build-essential
fi

`which co > /dev/null`
if [ $? -eq 0 ] ;then
        echo " RCS instalado"
else
        echo "Instalando RCS"
        apt-get install rcs
fi

`which xgettext > /dev/null`
if [ $? -eq 0 ] ;then
        echo " getText instalado"
else
        echo "Instalando gettext"
        apt-get install gettext
fi

`which autoconf > /dev/null`
if [  $? -eq 0 ] ;then
        echo " autoconf instalado"
else
        echo "Instalando autoconf"
        apt-get install autoconf
fi

`automake --version | head -n 1 | grep 1.6.3 > /dev/null`
if [ $? -eq 0 ] ;then
        echo " automake 1.6.3 instalado"
else
        echo "Instalando automake 1.6.3"
        tar -xzf automake-1.6.3.tar.gz
        cd "$ruta"/automake-1.6.3
        "$ruta"/automake-1.6.3/configure && make && make install
        cp "$ruta"/automake-1.6.3/automake /usr/local/bin
        rm -rf automake-1.6.3
fi
```

```
cd "$ruta"/"$whois"
echo "Instalando el servidor whois"
"$ruta"/"$whois"/configure && make && make install

`which in.swhoisd > /dev/null`
if [  $? -eq 0 ] ;then
        echo "Servidor whois instalado correctamente /usr/bin/in.swhoisd"
else
        echo "No se pudo generar el servidor in.swhoisd. Verificar "
        exit 1
fi

echo "Agregando el script swhoisd en /etc/init.d"
cp "$ruta"/"$parser"/swhoisd /etc/init.d/

echo "Instalando una base de datos actualizada al 1 de marzo del 2011"
cd "$ruta"/"$parser"
"$ruta"/"$parser"/whois.pl

/etc/init.d/swhoisd start
if [ -e /etc/init.d/swhoisd ]; then
        echo "Configurando whois como un servicio de inicio en /etc/rcS.d con
   prioridad 80"
        ln -s /etc/init.d/swhoisd /etc/rcS.d/S80whois
else
        echo "Ocurrió un error al copiar el archivo swhoisd en /etc/init.d"
fi

echo "Consulta el archivo LEEME. Para actualizar la base de datos es necesario
   configurar las variables depen y salida del archivo whois.pl"
```

3.8. Documentación

Para proveer facilidad y claridad en la instalación, configuración y uso del servidor whois, desarrollé el archivo LEEME.txt, el cual incluí en el archivo whoisUNAM.tgz de la aplicación de manera que si en el futuro ésta necesita ser reinstalada, se tenga un documento de referencia que permita a otros miembros del UNAM-CERT instalarla y configurarla.

Durante mi desarrollo profesional y académico he notado que muchos desarrolladores no documentan el software, lo que causa confusión en el uso de las aplicaciones y en el peor de los casos, que estos sistemas dejen de utilizarse.

A continuación incluyo el archivo LEEME.txt:

```
Instalación
Ejecutar el archivo de instalación:
./instalar

Se instalará una base de datos no actualizada del SAI, con el objetivo de probar
   la funcionalidad del servidor. Será necesario modificar las variables depen y
```

salida del archivo whois.pl en función de la ubicación deseada y configurar el envío programado del archivo de las dependencias para que la base de datos whois se actualice diariamente.

El archivo de entrada es la lista de los administradores del SAI, separada por el delimitador pipe |.

El archivo de salida lee el archivo de entrada y genera el archivo de salida correspondiente en un formato que pueda reconocer el servidor swhoisd. Este archivo es ubicado en el archivo /etc/swhoisd.conf

Para actualizar la base de datos será necesario obtener la información del SAI diariamente de la siguiente forma:

1.- Establecer una relación de confianza entre el servidor donde se encuentra el SAI y el servidor whois.

2.- Modificar el script whois.pl para leer el archivo de entrada después de que es enviado por el servidor del SAI. En el mencionado script se ubican claramente las variables depen y salida que deben ser configuradas.

3.- Ejecutar diariamente con una tarea programa el script whois.pl, para actualizar la base de datos de los administradores tomando como entrada el archivo que se enviado por el servidor del SAI.

Para realizar la tarea programada se puede ejecutar un cronjob. Para agregar una nueva tarea, ejecutar:

```
crontab –e
```

Para ejecutar el programa por ejemplo diariamente a las 2:30, se debe agregar la siguiente línea:

```
# minuto hora diaDelMes mes diaDeLaSemana(domingo=0) Comando
30 14 * * * /home/whois/ParseaSAI/whois.pl
```

FILTRADO DE TRÁFICO

Se pueden utilizar mecanismos a nivel de red o de host para filtrar el tráfico, a continuación se proveen líneas de iptables que permiten filtrar las peticiones ya sea en el servidor whois o en un firewall de red que ejecute iptables.

Para restringir que se conecten solo determinadas IPs al puerto 43

```
$externa=132.248.2.1 #IP del Departamento de Redes autorizada para realizar peticiones.
$in=132.248.1.1 #IP del servidor whois
# Segmento de la red interna autorizada
A INPUT -s 132.248.124.0/24 -d $in/32 -p tcp—dport 43 -j ACCEPT
A INPUT -s $externa/24 -d $in/32 -p tcp—dport 43 -j ACCEPT
A INPUT -s 0/0 -d $in/32 -p tcp—dport 43 -j DROP
```

Usar los programas iptables-restore e iptables-save para agregar las reglas a la configuración existente.

ADMINISTRACION DEL SERVIDOR

Para iniciar, detener, reiniciar y ver el estado del servidor whois, se debe usar el script

swhois ubicado en /etc/init.d

Iniciarlo: /etc/init.d/swhoisd start o simplemente /etc/init.d/swhoisd

Detenerlo: /etc/init.d/swhoisd stop

Reiniciarlo: /etc/init.d/swhoisd restart

Ver el estado: /etc/init.d/swhoisd status

EJECUCIÓN AL INCIO DEL SISTEMA

Agregar una liga suave en la ubicación /etc/rcS.d

```
ln -s /etc/init.d/swhoisd S80whois
```

3.9. Actualización de la información

La información de los administradores de la red se actualiza en el Sistema de Atención a Incidentes. La jefatura del departamento de respuesta a incidentes del UNAM-CERT determinó que se realizara la actualización de la información del servidor whois diariamente. Para ello, se estableció una relación de confianza, mediante la cual, el sistema que contiene la información del SAI envía un archivo al servidor whois, el cual posteriormente aplica el formato necesario a la información para que sea reconocida por la aplicación whois.

Sistema de Atención de Incidentes

1. Generar el par de claves en el servidor que contiene el SAI
   `# ssh-keygen –t rsa`
2. Asignar un passphrase con una clave robusta. (Se almacenan las claves en el directorio `/home/<usuario>/.ssh/)`
3. Enviar la clave pública al servidor whois, para que el servidor SAI pueda enviar la información automáticamente.
   `# scp /home/<usuario>/.ssh/id_rsa.pub <usuario>@<IP del servidor>:.ssh/authorized_keys`
   Luego de crear la relación de confianza en el servidor del Sistema de Atención de Incidentes, se establece una tarea programada para enviar la bitácora diariamente.

```
$ crontab –e
```

Se agrega la siguiente línea:

```
31 15 * * * scp <ruta absoluta>/dependencias <usuario>@<s. whois>:Dependencias
```

Por último se crea una tarea programada en el servidor whois, para leer el archivo enviado por el servidor SAI y generar el archivo en un formato reconocible por el servidor whois.

```
30 15 * * * /home/whois/ParserSAI/whois.pl
```

Script para leer los archivos recibidos del Sistema SAI que genera la base de datos `/etc/swhoisd` para que pueda ser reconocida por el servidor whois.

3.9.1. Script de generación de la base de datos

El script whois.pl, escrito en lenguaje perl, es responsable de leer los archivos recibidos del Sistema SAI que genera la base de datos `/etc/swhoisd`, la cual es consultada por el servidor swhoisd cuando recibe peticiones. El contenido de este archivo se muestra a continuación.

```
#!/usr/bin/perl
$usuario=incidentes
$depen=”/home/$usuario/whoisUNAM/dependencias_”.‘date +%y%m%d.txt‘;
$salida= “/home/$usuario/whoisUNAM/bdepen_”.‘date +%y%m%d.txt‘;
$t=0;
$cont_dep=0;
open(D,”<$depen”);
open(S,”>$salida”);
```

```
while (my $linea = <D>){
chomp($linea);

@datos=split('\\|',$linea);## se separa el archivo por |
chomp($datos);
$cont=0;
$cont2=0;
$ip=0;
$num_cont=0;
$num_datos=$#datos;

if(($a =~ /(\\|(\d{1,3})*)/ ) && ($num_datos >1)){
foreach $a (@datos){
if (($a =~ /(^[a-zA-Z]\w)/) && ($cont == 0)){
$nom_dep=$a;
$cont_dep++;

                        }
if ($a =~ /((\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3}))/){
$ips{$a}++;
                        }
if (($a =~ /(\\|[a-zA-Z]\w)/) && ($cont > 1)){
$contac[$num_cont]=$a;
@info_contac=split(',',$contac[$num_cont]);
foreach $inf (@info_contac){
if (($inf =~ /(^[a-zA-Z]\w)/) && ($inf !~ /[a-zA-Z]+[\w]*\@[a-zA-Z]+[\w]*/)){
$nomb_cont=$nomb_cont." ".$inf;
                                        }
if($inf =~ /(^&\w)/){
@quita=split("&",$inf);
$pue=$quita[1];
                                        }
if ((($inf =~ /^[0-9]/) || ($inf =~ /^\([0-9]/)) && ($inf !~ /[a-zA-Z]+[\w]*\@[a-
zA-Z]+[\w]*/)) {
$telefonos=$telefonos." ".$inf;
                                        }
if ($inf =~ /[a-zA-Z]+[\w]*\@[a-zA-Z]+[\w]*/){
$correos=$correos." ".$inf
                                        }
                                    }

$nombres[$num_cont]=$nomb_cont;
$email[$num_cont]=$correos;
$fones[$num_cont]=$telefonos;
$puesto[$num_cont]=$pue;
$nomb_cont=();
$correos=();
$telefonos=();
$num_cont++;

                        }

$cont++;
                }
```

```
foreach $rangos (keys%ips){
#print
   "Rangos++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   ++++++++++++: $rangos\n";
@ran=split("\\.",$rangos);
@oct4=split(",",$ran[3]);
($ini,$fin)=split("-",$oct4[1]);
#print "inicio: $ini  fin: $fin\n";
$num_ip=1;
for($i=$ini;$i<=$fin;$i++){
print S "\n\nDepe$cont_dep nr {";
#print S "\n ns1ip $oct4[1]";
print S "\n !address $ran[0].$ran[1].$ran[2].$i";
print S "\n !name $nom_dep";
for ($j=0;$j<$num_cont;$j++){
$m=$j+1;
print S "\n contact ($m)$nombres[$j], $puesto[$j]";
print S "\n phone $fones[$j]";
print S "\n email $email[$j]";
                                          }
print S "\n}";
$num_ip++;
                                  }

                  }


%ips = ();
        }

   }
close(S);
close(D);
```

3.9.2. Script de actualización de base de datos

Este programa a su vez ejecuta el script whois.pl y permite verificar si se recibió o no. Escribe en una bitácora si detectó o no el archivo del servidor en donde se encuentra el sistema SAI, lo que permite detectar errores rápidamente y detectar puntos de fallas.

```
#!/bin/bash

# David Bernal

ruta=/home/whois
base=$ruta/DepenSAI/dependencias_`date +%y%m%d.txt`
salida=$ruta/BaseDepen/bdepen_`date +%y%m%d.txt`

if [ ! -f "$base" ];then
        echo " `date` SWHOISD: no existe la base del SAI "$base" " >> $ruta/log
        exit 1
else
```

```
        mv "$base" $ruta/Cdepen
        $ruta/whoisUNAM/ParserSAI/whois.pl
        if [ $? -eq 0 ];then echo " `date` SWHOISD: base de datos "$base"
   actualizada" >> $ruta/log;
        fi
        #rm $ruta/Cdepen
        cp "$salida" /etc/swhoisd.conf
fi
```

3.9.3. Tareas programadas

La configuración de una tarea de cron permite actualizar, diaria y automáticamente, la información que se envía desde el servidor en el que se encuentra almacenado el SAI. Para agregar una tarea, se ejecuta el siguiente comando:

```
# crontab –e
```

Se agrega la siguiente línea:

```
# m h dom mon dow command
00 18 * * * /home/whois/whoisUNAM/ParserSAI/actualizaWhois.sh
```

3.10. Pruebas de funcionamiento

```
$ whois –h <servidor de whois> <patrón de búsqueda>
```

En la figura 3.2 se muestra la ejecución de la consulta al servidor whois mediante una dirección IP que pertenece a la Facultad de Ingeniería.

```
debian:/usr/src/whoisUNAM/ParserSAI# whois -h whois 132.248.52.1

               SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT


RedUNAM                   (Dependencia Depe31)
-------------------------------------------------------------------------------
Patrón de búsqueda:     132.248.52.1
Dependencia:              FACULTAD DE INGENIERÍA
Contacto:                 (1) Noé Cruz Marín, Jefe del departamento de cómputo avanzado
Teléfono:                5622 0951
Email:                    noecm@cancun.fi-a.unam.mx
Contacto:                 (2) Rafael Sandoval Vázquez, Jefe del Departamento de Seguridad en Cómputo
Teléfono:                5622 0925
Email:                    rafael@seguridad.fi-a.unam.mx
Contacto:                 (3) Enrique Barranco Vite, Jefe de la Unidad de Cómputo Académico
Teléfono:                5622 0951 5622 0955
Email:                    barranco@cancun.fi-a.unam.mx
Red:                      132.248.54.0,1-254|132.248.59.0,1-254|132.248.139.0,1-254|132.248.52.0,1-254
```

Fig. 3.2 Ejecución de la consulta al servidor whois mediante una dirección IP.

REFERENCIAS DEL CAPÍTULO

[1] http://www.rfc-editor.org/, Sitio que contiene documentos del tipo RFC publicados por la IETF, 7 de mayo de 2011.

[2] http://www.faqs.org/rfcs/rfc3912.html, Documento RFC 3913, la más reciente del documento RFC del protocolo whois, 7 de mayo de 2011.

[3] http://www.faqs.org/rfcs/rfc954.html, Documento RFC 954, RFC en desuso del protocolo whois, 7 de mayo de 2011.

[4] http://www.rfc-editor.org/rfc/rfc1834.txt Documento RFC 954, RFC en desuso del protocolo whois, 7 de mayo de 2011.

[5] http://aso.icann.org/internet-community/regional-internet-registries-rirs/, Sitio de ICAN(IANA) con la lista de organizaciones regionales de asignación de números de Internet, 7 de mayo de 2011.