4. CAPÍTULO CUATRO - RESULTADOS OBTENIDOS

Después de algunas semanas de que el servidor whois estuvo en funcionamiento, consideré que podía extenderse su funcionalidad para ser de mayor utilidad a miembros de respuesta a incidentes. Propuse que la aplicación fuera modificada para que el servidor whois proporcionara información de equipos de respuesta a incidentes de seguridad en cómputo (CERTS) alrededor del mundo, con el fin de dar una respuesta más rápida a incidentes de seguridad en cómputo ocurridos en otros países.

También planteé que se permitiera buscar una dependencia por nombre, debido a que en muchas ocasiones los miembros de respuesta a incidentes requieren determinar los segmentos asignados a una dependencia o datos de sus administradores y no cuentan con una dirección IP para realizar la consulta. El jefe de respuesta a incidentes consideró convenientes las propuestas y me autorizó realizar los cambios.

Así mismo, modifiqué el código fuente para que el sistema mostrara palabras con acentos, mediante la codificación de las letras con acento en Unicode en el código fuente `src/do_whois.c` con la sintaxis: `\uXXXX` en las cadenas de las sentencias de impresión de texto.

Realicé una segunda versión del archivo de generación de la base de datos, el código de ésta se detalla en la siguiente sección.

4.1. Segunda versión del archivo actualizaWhois.sh

```
#!/bin/bash
# David Bernal
# Por una relación de confianza entre el servidor del SAI y el servidor whois,
# se escriben automáticamente las bitácoras de dependencias en la carpeta
# BaseDepen de whois.

# Esta versión agrega la información de los CERTs en la BD, imprime palabras
# con acento y permite buscar dependencias por nombre.
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

        cat $ruta/certs > $ruta/Cdepen; grep "|.*|.*|" "$base" |  awk -F "|" '{
   print length($1) ,$0 }' | sort -n | awk '{$1="";print $0}' >> $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
```

4.2. Segunda versión del archivo whois.pl

También modifiqué el archivo de creación de la base de datos whois.pl con el fin de diferenciar los registros de los CERTS de los registros de Dependencias de la UNAM y mostrarlos en un formato diferente. Debido a la extensión del archivo whois.pl a continuación sólo se incluye el bloque de código modificado:

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

    @datos=split('\\|',$linea);## se separa el archivo por |
    chomp($datos);
    $nom_dep=$datos[0];

    if( $nom_dep =~ /CERT-/ ){
          print S "\n\nDepe$cont_dep nr {";
          print S "\n !name $nom_dep";

       for($i=1;$i<=$#datos;$i++){
           @cert = split(',',$datos[$i]);
           print S "\n contact ($i)$cert[0]";
           print S "\n phone $cert[1]";
           print S "\n email $cert[2]";
           print S "\n red $cert[3]";
       }

       print S "\n}";
       $cont_dep++;
       next;
    }
…
```

Para agregar la información de CERTS en la base de datos, basta escribir la información de cada uno de los equipos de respuesta a incidentes en el archivo CERTS ubicado en el directorio definido en el parámetro `$ruta` del script del archivo de actualización `actualizaWhois.sh`. Cada registro debe tener el siguiente formato:

```
CERT-<país> | <nombre del CERT 1>, <teléfonos>, dirección de correo, página web |
  <nombre de Cert2> …
```

Es posible agregar múltiples CERTs para un país, como es el caso de Estados Unidos, basta separarlos con tabulador.

```
CERT-US | US-CERT, +1-703-235-5111, soc@us-cert.gov - phishing-report@us-
  cert.gov, http://www.us-cert.gov | CERT/CC, +1-412-268-7090, cert@cert.org,
  http://www.cert.org/
```

En la figura 4.1 se muestra la ejecución de la consulta al servidor whois para mostrar los datos de contacto del CERT de Argentina.

```
debian:/usr/src/whoisUNAM# whois -h whois CERT-AR

               SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT



RedUNAM                   (Dependencia Depe0)
-------------------------------------------------------------------------
Dependencia:              CERT-AR
Contacto:                 (1) ArCERT
Teléfono:                +54-11-4345-0383
Email:                    mailinfo@arcert.gov.ar
Red:                      http://www.arcert.gov.ar
```

Fig. 4.1 Ejecución de la consulta del CERT de Argentina

En caso de que haya más de un CERT por país, como es el caso de Estados Unidos en donde se encuentra el US-CERT y también el CERT/CC se realiza tal y como se indica en la figura 4.2

```
debian:/usr/src/whoisUNAM# whois -h whois CERT-US

               SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT



RedUNAM                   (Dependencia Depe1)
-------------------------------------------------------------------------
Dependencia:              CERT-US
Contacto:                 (1) US-CERT
Teléfono:                +1-703-235-5111
Email:                    soc@us-cert.gov
Red:                      http://www.us-cert.gov
Contacto:                 (2) CERT/CC
Teléfono:                +1-412-268-7090
Email:                    cert@cert.org
Red:                      http://www.cert.org/
```

Fig. 4.2 Ejecución de la consulta de los CERTs de Estados Unidos

También modifiqué el sistema para que se pudieran realizar consultas por nombre de dependencia, como se muestra en la figura 4.3.

```
debian:/usr/src/whoisUNAM/ParserSAI# whois -h localhost UNAM-CERT

                SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT



RedUNAM                   (Dependencia Depe23)
-------------------------------------------------------------------------------
Patrón de búsqueda:     unam-cert
Dependencia:              DGTIC, SSI/UNAM-CERT
Contacto:                 (1) Rubén Aquino Luna, Subdirector de Seguridad de la Información
Teléfono:                56228169
Email:                    raquino@seguridad.unam.mx
Contacto:                 (2) Roberto Sánchez Soledad, Responsable del Área de Atención a Incidentes
Teléfono:                56228169
Email:                    rsanchez@seguridad.unam.mx
Red:                      132.248.124.0,124-192
```

Fig. 4.3 Ejecución de la consulta por nombre de dependencia

Las modificaciones realizadas permitieron obtener como resultado un sistema con las siguientes características:

- *Facilidad de administración* – Realicé un script de administración especialmente desarrollado para el Sistema Operativo objetivo, Debian 5.
- *Claridad* – Se proporciona documentación que indica claramente cuál es la función de cada uno de los elementos del sistema y se define cuáles fueron los cambios realizados.
- *Facilidad de instalación* – Realicé un script auto instalador que ejecuta todas las acciones necesarias el cual permitirá migrar fácilmente el servidor whois a otra computadora en caso de ser necesario.
- *Flexibilidad* – El servidor whois puede proporcionar información de dependencias de la UNAM por dirección IP o nombre de la dependencia, además permite agregar y consultar información de equipos de respuesta a incidentes mediante el código del país.
- *Extensibilidad* – Debido a que la información es accesible por terminal mediante un cliente whois, es posible crear programas que utilicen la información del servidor whois, funcionalidad con la que no cuenta, en este momento, el Sistema de Atención a Incidentes (SAI)