Practica 2: CSIRTs Parte 1

NOTIFICACIÓN - Puntos de contacto asociados a direcciones IP

Cuando una organización necesita direcciones IP, debe solicitar un bloque IP a un RIR o Registro Regional de Internet. Estas solicitudes, dependiendo de la región geográfica en la que la organización se encuentre, deben ser realizadas al RIR que opera en la región geográfica donde la organización se encuentre. Existen cinco RIRs que se distribuyen su área de cobertura de la siguiente manera:

- AfriNIC: Región de África
- APNIC: Región de Asia Pacífico
- ARIN: Región de América del Norte y varias islas del Caribe y del Atlántico Norte
- LACNIC: Región de América Latina y el Caribe
- RIPE NCC: Europa, Oriente Medio y parte de Asia Central

Algunos países se reservan la autonomía de asignar recursos IP en su territorio. En estos países funcionan lo que se llaman NIRs o Registros Nacionales de Internet. En estos casos, el RIR es quien le brinda recursos de Internet (direcciones IP y números de sistemas autónomos) a los NIRs para que éstos realicen la asignación a los registrantes de su territorio.

Actualmente los NIRs que operan en la región del RIR LACNIC son:

- Brasil
- México

Actualmente los NIRs que operan en la región del RIR APNIC son:

- China
- India
- Indonesia
- Japan
- Korea
- Taiwan
- Vietnam

Datos brindados por los RIR asociados a recursos IP asignados

Dado que la información de asignación de bloques de direcciones IP es información pública, la misma puede ser obtenida utilizando distintos protocolos de consulta. Los registros públicos brindan información sobre la organización que tiene un bloque IP asignado, incluyen:

- Organización que realizó el registro.
- Nombre de la organización.
- Dirección postal.
- País.
- Teléfonos de contacto.
- Distintas direcciones de correo electrónico de contacto, las cuales estan asociadas a distintos roles:
    - Registrant
    - Administrativo
    - Técnico
    - Abuse
- Fechas asociadas a la creación y modificación de los datos.

Un CSIRT a la hora de contactar a una organización para reportar un incidente de seguridad utilizará preferentemente el contacto de abuse.

Herramientas de consulta de información pública: WHOIS / RDAP

Existen distintas interfaces de acceso a información de contacto sobre quienes son los propietarios o registrantes de una dirección IP, un número de Sistema Autónomo o un nombre de dominio:

- Originalmente se utilizaba el protocolo WHOIS para consultar información de contacto sobre distintos tipos de recursos gestionados por diferentes organizaciones.
- En el año 2015 se estandarizó el protocolo RDAP (Protocolo de Acceso a Datos de Registro). A diferencia de WHOIS, RDAP utiliza una estructura determinada para el almacenamiento de la información de contacto. Esto lo hace más adecuado para ser usado en procesos de extracción de datos automatizados.
- Diversos portales web permiten realizar este tipo de consultas, utilizando una interfaz de usuario más amigable. Estos portales utilizan protocolos como WHOIS o RDAP para obtener la información consultada.

Para consultar utilizando el protocolo WHOIS o el protocolo RDAP es necesario utilizar un cliente de WHOIS o RDAP según sea el caso. El cliente de WHOIS está más difundido y

habitualmente ya se encuentra instalado o viene paquetizado para ser instalado en la mayoría de los sistemas operativos.
Para el caso de RDAP, es posible encontrar distintos clientes que se pueden instalar en el sistema. Entre los más conocidos podemos mencionar:

- NicInfo - es un cliente RDAP escrito por ARIN
  - https://www.arin.net/resources/registry/whois/rdap/#rdap-client
  - https://github.com/arineng/nicinfo
- OpenRDAP - un cliente RDAP escrito en GO
  - https://www.openrdap.org/
  - https://github.com/openrdap/rdap

Es importante mencionar, que de una organización en la base de datos de WHOIS puede no ser consistente con la encontrada en la base de datos RDAP. Para la consulta de recursos IP, RDAP suele tener información más precisa y actualizada.

Ejercicio 01 (Usar cliente RDAP)

Para cada una de las siguientes direcciones IP indique **el mail de contacto** que considere más adecuado para para reportar un incidente de seguridad proveniente desde dicha dirección IP:

a. 218.234.18.106
b. 70.240.222.159
c. 200.204.153.97
d. 85.63.113.123
e. 163.10.53.96
f. 54.36.96.8

Ejercicio 02

Una LEA (Law Enforcement Agency) necesita contactar al RIR o el NIR que mantiene los registros de la asignación de los siguientes recursos IP con el objeto de solicitar a los mismos información adicional sobre las organizaciones registrantes.
Para cada una de las siguientes, indique el RIR (AFRINIC, ARIN, APNIC, LACNIC o RIPE) o NIR (indicar el País) que realizó la asignación:

a. 218.234.18.106

b. 70.240.222.159
c. 200.204.153.97
d. 85.63.113.123
e. 163.10.53.96
f. 54.36.96.8

NOTIFICACIÓN - Puntos de contacto asociados a nombres de dominio

---

ICANN[1] es una organización sin fines de lucro que opera a nivel internacional, entre otras, responsable de las funciones de gestión del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD), así como de la administración del sistema de servidores raíz (root servers).

En relación al DNS, ICANN es responsable de la coordinación de la administración de los elementos técnicos del DNS para garantizar una resolución unívoca de los nombres, de manera que los usuarios de Internet puedan encontrar todas las direcciones válidas. Para ello, se encarga de supervisar la distribución de los identificadores técnicos únicos usados en las operaciones de Internet, y delegar los nombres de dominios de primer nivel (como .com, .info, etc.).

En la gestión de los nombres de dominios ICANN establece políticas que deben cumplirse en el proceso de registración de dominios. En este proceso aparecen distintos tipos de actores que, luego de definirlos, se utilizará su denominación en inglés para evitar confusiones:

- **Registrante** o **Registrant**: Persona o entidad que requiere el registro de un nombre de dominio. Luego del registro, el **registrant** tiene un contrato con el **registrar**.

- **Registrador** o **Registrar**: Una organización a través de la cual un **registrants** puede realizar el registro de un nombre de dominio. Durante el proceso de registro, el **registrar** verifica que el nombre de dominio requerido cumpla con requerimientos del **registry** y realiza el requerimiento con el **operador del registry**. Los **registrars** son responsables

[1] ICANN - Internet Corporation for Assigned Names and Numbers - https://www.icann.org/

de obtener información de los **registrants** y hacerla disponible a través de servicios de consulta como WHOIS. Luego del registro de un nombre de dominio, el **registrant** gestiona cualquier cambio a través del **registrar**. El **registrar** será quien tenga que enviar los cambios requeridos por el **registrant** al **registry**.

- **Registro** o **Registry**: repositorio autoritativo sobre la información de un TLD en particular. Cada TLD está asociado con un **registry** que contiene los registros de cada nombre de dominio que existe en ese dominio. El DNS utiliza esta información para determinar los servidores de nombres asociados a los distintos nombres de dominio registrados en ese TLD. El **operador del registry** es la organización encargada de mantener el repositorio autoritativo de un TLD en particular.

En resumen, podemos decir que, para cada TLD, habrá:

- Una organización encargada de realizar las funciones de operación del **registry**. La información sobre las organizaciones encargadas de gestionar el **registry** de los TLD, tanto gTLP como ccTLD, se puede consultar en: https://www.iana.org/domains/root/db.
- Una o más organizaciones encargadas de realizar funciones de **registrar**.

En el caso de Argentina, tanto las funciones de registry como de registrar las lleva a cabo NIC.ar

Herramientas de consulta de información pública: WHOIS / RDAP

En el sistema de nombres de dominio, la gestión de la información pública es mantenida por:

- El **registry** de cada uno de los TLD.
- El **registrar** que vendió el dominio al **registrant**.

Dado un TLD, en el **registry** se puede obtener información pública sobre:

- Fechas de asignación del dominio.
- Fecha de expiración del dominio.
- Fecha de actualización de los datos del registro.
- **Registrar** que vendió el dominio.
- Datos de contacto del **registrar.**
- Datos del servicio de consultas implementado por el **registrar.**

En el servicio de consulta implementado por un **registrar** que opera vendiendo dominios de un TLD, se pueden encontrar:

- Datos del **registrant** (persona u organización que realizó la compra del dominio).

- Datos de contacto sobre el **registrant**.
  En muchos casos el **registrar** brinda al **registrant** la posibilidad de proteger su privacidad. Esto deriva en que los datos que se tendrán del **registrar** serán direcciones de correo electrónico o formularios web del propio **registrar**.

Las herramientas de consulta, tanto WHOIS como RDAP, utilizan el servicio de consulta del **registry** del TLD consultado y luego consultan el servicio de WHOIS o RDAP provisto por el **registrar** del dominio buscado.

Es preferente utilizar el cliente de WHOIS. La razón de esto es que generalmente, la información alojada en los REGISTRARs, aún no fue migrada.

Ejercicio 03 (Usar cliente WHOIS)

Para cada uno de las siguientes nombres de dominio indique el punto de contacto definido (**mail o URL)** que utilizaría para comunicarse con la organización que registró el dominio.

A. google.com
B. noticiasdeinternet.net
C. clarin.com
D. perfil.com
E. cualesmiip.com

Ejercicio 04

Una LEA (Law Enforcement Agency) necesita contactar al REGISTRAR que realizó la asignación de los siguientes nombres de dominio con el objeto de solicitar información adicional sobre el REGISTRANT.
Para cada uno de las siguientes nombres de dominio indique el mail de contacto para cuestiones de abuso del REGISTRAR que utilizaría para comunicarse con la organización que vendió el dominio.

A. google.com
B. noticiasdeinternet.net
C. clarin.com

D. perfil.com
E. cualesmiip.com