

Alumno: Rodrigo Vila

## **Ejercicio número 1 - Unidad 2**

Crear un informe explicando que son las bases de datos "WHOIS" y cuáles son las correspondientes a nuestra zona (continente) y país.

**Informe sobre Bases de Datos WHOIS y sus Correspondientes en Argentina:**

### **Introducción:**

Las bases de datos WHOIS son herramientas fundamentales en el ámbito de Internet que proporcionan información sobre la titularidad y los detalles de contacto asociados con los nombres de dominio, direcciones IP y otros recursos de Internet. El término "WHOIS" proviene del inglés "Who is?", que significa "¿Quién es?".

### **Funcionamiento de WHOIS:**

La información contenida en una base de datos WHOIS incluye datos como el nombre del titular del dominio, la organización a la que pertenece, la dirección postal, el correo electrónico, el número de teléfono y los servidores de nombres asociados con el dominio. Esta información es pública y puede ser consultada por cualquier persona a través de herramientas de búsqueda WHOIS disponibles en línea.

### **Utilidad de WHOIS:**

Las bases de datos WHOIS son utilizadas por una variedad de actores en Internet, incluidos registradores de dominios, empresas de alojamiento web, agencias gubernamentales, investigadores de seguridad informática y particulares interesados en la información de registro de un dominio.

### **Bases de Datos WHOIS en Argentina:**

En Argentina, el ente encargado de administrar los nombres de dominio bajo el dominio de nivel superior de código de país (ccTLD) ".ar" es la Asociación Argentina de Registro de Internet (NIC Argentina). NIC Argentina opera su propio servicio de búsqueda WHOIS que proporciona información sobre los nombres de dominio registrados bajo el dominio ".ar".

### **NIC Argentina WHOIS:**

El servicio de búsqueda WHOIS de NIC Argentina se encuentra disponible en su sitio web oficial. Permite a los usuarios buscar información sobre los nombres de dominio registrados bajo el ccTLD ".ar". La información proporcionada incluye detalles sobre el titular del dominio, los servidores de nombres asociados y la fecha de registro, entre otros datos relevantes.

### **Conclusiones:**

Las bases de datos WHOIS son una herramienta crucial para obtener información sobre los nombres de dominio y otros recursos de Internet. En Argentina, NIC Argentina es el organismo encargado de administrar el ccTLD ".ar" y proporciona un servicio de búsqueda WHOIS para acceder a la información de registro de los dominios bajo su jurisdicción.

En América del Sur, cada país tiene su propio organismo encargado de administrar los nombres de dominio bajo su dominio de nivel superior de código de país (ccTLD). Por lo tanto, hay múltiples bases de datos WHOIS, una por cada ccTLD de cada país en la región. Por ejemplo:

En Chile: ".cl" - Administrado por el NIC Chile, perteneciente a la Universidad de Chile.

En Brasil: ".br" - Administrado por el Comitê Gestor da Internet no Brasil (CGI.br) a través del Registro.br.

En Perú: ".pe" - Administrado por la Red Científica Peruana (RCP).

Entre otros.

## **Ejercicio número 2 - Unidad 2**


**Buscar en Internet 4 direcciones IP y examinarlas. Transformar a las mismas en binario.**

**Utilizando en Windows 10 el comando "ping -4 www.google.com" obtengo:**

Dominio: www.google.com

IP: 142.250.79.100

Realizando un whois en "www.whois.com/whois" obtengo:

 Domain Information	
Domain:	google.com
Registrar:	MarkMonitor Inc.
Registered On:	1997-09-15
Expires On:	2028-09-13
Updated On:	2019-09-09
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

 Registrant Contact	
Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at <a href="https://domains.markmonitor.com/whois/google.com">https://domains.markmonitor.com/whois/google.com</a>

## Transformo la IP 142.250.79.100 a numero binario:

Convierto cada octeto a su representación binaria de 8 bits:

1. 142 en binario es 10001110
2. 250 en binario es 11111010
3. 79 en binario es 01001111
4. 100 en binario es 01100100

Entonces 142.250.79.100 en binario es: 10001110.11111010.01001111.01100100


Utilizando en Windows 10 el comando "ping -4 www.elhacket.net" obtengo:

Dominio: www.elhacker.net

IP: 104.26.4.20

Realizando un whois en "www.whois.com/whois" obtengo:

## elhacker.net

Updated 1 second ago 

Domain Information	
Domain:	elhacker.net
Registrar:	CloudFlare, Inc.
Registered On:	2001-02-22
Expires On:	2027-02-22
Updated On:	2022-11-24
Status:	clientTransferProhibited
Name Servers:	lily.ns.cloudflare.com sri.ns.cloudflare.com

Registrant Contact	
State:	Barcelona
Country:	ES
Email:	<a href="https://domaincontact.cloudflare.com/elhacker.net">https://domaincontact.cloudflare.com/elhacker.net</a>

### Transformo la IP 104.26.4.20 a numero binario:

Convierto cada octeto a su representación binaria de 8 bits:

1. 104 en binario es 01101000
2. 26 en binario es 00011010
3. 4 en binario es 00000100
4. 20 en binario es 00010100

Entonces 104.26.4.20 en binario es 01101000.00011010.00000100.00010100

Utilizando en Windows 10 el comando "ping -4 www.facebook.com" obtengo:

Dominio: www.facebook.com

IP: 31.13.94.35

Realizando un whois en "www.whois.com/whois" obtengo:

## facebook.com

Updated 4 hours ago 

Domain Information	
Domain:	facebook.com
Registrar:	RegistrarSafe, LLC
Registered On:	1997-03-29
Expires On:	2032-03-30
Updated On:	2023-04-26
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	a.ns.facebook.com b.ns.facebook.com c.ns.facebook.com d.ns.facebook.com

Registrant Contact	
Name:	Domain Admin
Organization:	Meta Platforms, Inc.
Street:	1601 Willow Rd
City:	Menlo Park
State:	CA
Postal Code:	94025

**Transformo la IP 31.13.94.35 a numero binario:**

Convierto cada octeto a su representación binaria de 8 bits:

1. 31 en binario es 00011111
2. 26 en binario es 00011010
3. 4 en binario es 00000100

4. 20 en binario es 00010100

Entonces 104.26.4.20 en binario es 01101000.00011010.00000100.00010100


**Utilizando en Windows 10 el comando "ping -4 www.youtube.com" obtengo:**

Dominio: www.youtube.com

IP: 172.217.172.78

Realizando un whois en "www.whois.com/whois" obtengo:

## youtube.com

Updated 1 day ago 

Domain Information	
Domain:	youtube.com
Registrar:	MarkMonitor Inc.
Registered On:	2005-02-15
Expires On:	2025-02-15
Updated On:	2024-01-14
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

Registrant Contact	
Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at <a href="https://domains.markmonitor.com/whois/youtube.com">https://domains.markmonitor.com/whois/youtube.com</a>

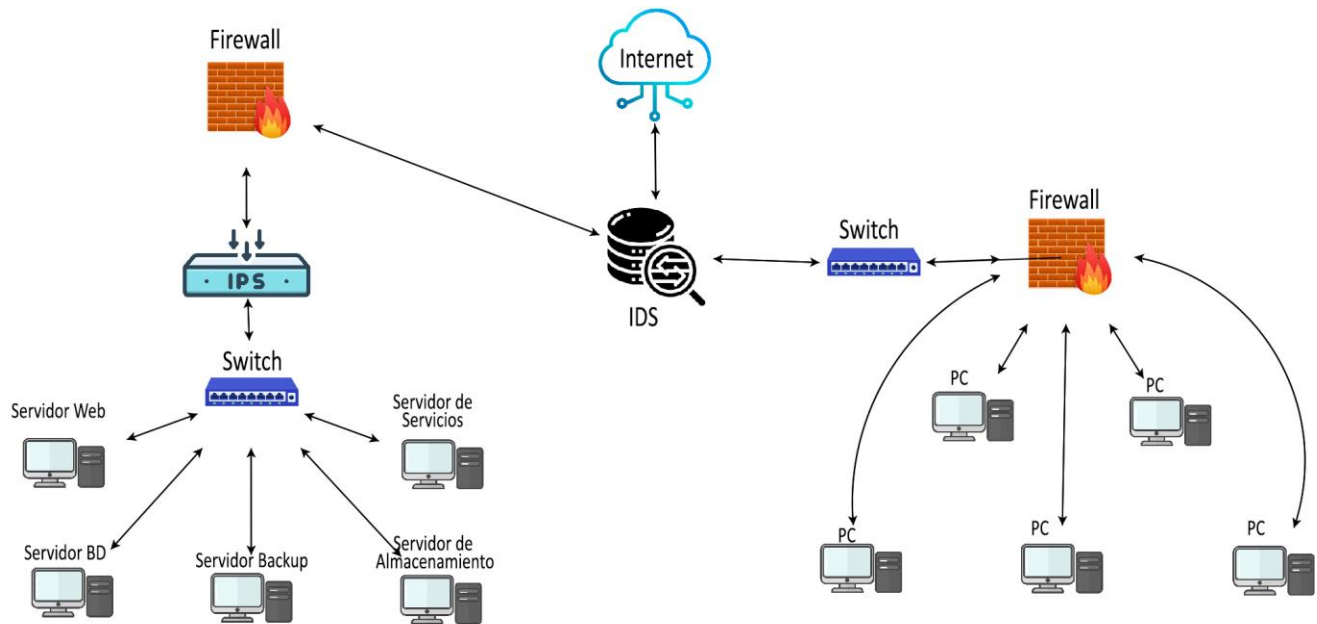
**Transformo la IP 172.217.172.78 a numero binario:**

Convierto cada octeto a su representación binaria de 8 bits:

1. 172 en binario es 10101100
2. 217 en binario es 11011001
3. 172 en binario es 10101100
4. 78 en binario es 01001110

Entonces 172.217.172.78 en binario es 10101100.11011001.10101100.01001110

## Ejercicio número 3 - Unidad 2



Seleccioné la Topologia estrella expandida por su versatilidad a la hora de agregar equipos o expandir la red, ademas de filtrar la seguridad del transito de red por orden de prioridad dandole mayor proteccion a los servidores.

La red consta de 2 subredes, que no estan conectadas entre si, obligando a las PC cliente a obtener informacion de los servidores pasando a traves de la seguridad de los IDS, firewall e IPS. (Como lo haria cualquier equipo externo), pero los dispositivos tendrian una configuracion de seguridad Restrictiva. Permitiendo el acceso a los servidores criticos solo a las IPs especificas de los equipos de la empresa.

Anotaciones que se tuvieron en cuenta en el armado de la red:

Dispositivos como: Firewall / IDS / IPS / NIDS / HIDS

Configurar ACL (Acces list) con las ips de los dispositivos de la red.

IDS (Intrusion Detection Systems)

NIDS: basado en hardware o software, protege la red entera

HIDS: basado en software, solo protege al equipo host

IPS: Intrusion Prevention System: deteccion en tiempo real, basada en firmas o en comportamientos de red. Configurable.

*Rodrigo Vila.-*