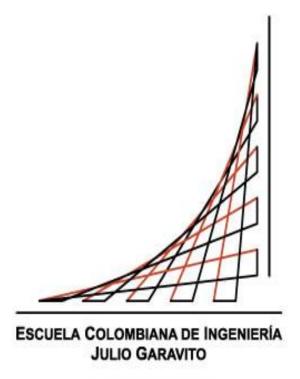
LABORATORIO 8 RECO



VIGILADA MINEDUCACIÓN

Miguel Angel Fuquene Arias

David Leonardo Coronado

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO BOGOTÁ D.C. 2 DE NOVIEMBRE 2020

Laboratorio No. 8 - capa de aplicación e infraestructura TI

Objetivo

Revisar la operación de protocolos de la capa de aplicación mediante la revisión de su operación y la instalación y configuración de algunos servicios típicos en una infraestructura TI empresarial.

Marco Teórico

Capa de aplicación:

La capa de aplicación es la séptima en el modelo OSI y es la que ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP).

Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar, pero los principales que se manejan en esta capa son los siguientes:

- FTP (File Transfer Protocol Protocolo Transferencia de Archivos) para transferencia de archivos.
- DNS (Domain Name Service Servicio de Nombres de Dominio)
- DHCP (Dynamic Host Configuration Protocol Protocolo Configuración Dinámica de Anfitrión)
- HTTP (HyperText Transfer Protocol) para acceso a páginas de internet.
- NAT (Network Address Translation Traducción de Dirección de Red)
- POP (Post Office Protocol) para correo electrónico.
- SMTP (Simple Mail Transport Protocol).
- SSH (Secure SHell)
- TELNET para acceder a equipos remotos
- TFTP (Trival File Transfer Protocol).

En general esta capa es la que hace posible que todos los protocolos que normalmente utilizamos en el ordenador (correo electrónico, navegar por páginas webs, etc.) funcionen correctamente.

Telnet:

Telnet es una herramienta que ha sido utilizada durante décadas por los administradores de sistema informáticos en el ámbito de las redes. Las conexiones remotas no son algo precisamente nuevo, ya desde las primeras redes y con sistemas sin escritorio se utilizaban herramientas como Telnet para conectarnos a servidores y equipos conectados a una red,

tanto de forma remota como interna.

El nombre de Telnet proviene del acrónimo Telecomunication Network, y básicamente un protocolo de red TCP/IP que es utilizado desde 1960 para establecer conexiones remotas con otros ordenadores, servidores, y dispositivos con un sistema compatible en el acceso mediante este sistema de comunicación. De forma predeterminada se utiliza el puerto de conexión 23.

Además del propio protocolo, también recibe este nombre el programa que lo utiliza para establecer la propia conexión. Para acceder a la otra máquina de forma remota, debemos utilizar un terminal, por ejemplo, Símbolo del sistema de Windows, o el Terminal de Linux. De esta forma podremos interactuar en la máquina remota navegando por sus archivos, ejecutando otros comandos internos, si tenemos permiso, y monitorizar el estado de la propia máquina sin la necesidad de ir físicamente al lugar en donde se encuentra.

HTTP

HTTP es la abreviación de Protocolo de Transferencia de Hipertexto y es un protocolo de aplicación para permitir la comunicación entre sistemas físicamente dispersos.

Fue originalmente ideado por Sir Tim Berners Lee en 1989. Ahora está coordinado por el W3C.

En su formato más básico, es lo que establece cómo las páginas web se comunican desde el servidor web al navegador del usuario.

El Hipertexto es el texto que se usa en las páginas web y que conecta una página con otra, ya sea dentro del mismo sistema o externamente. Son los enlaces que conectan el contenido en Internet.

HTTP es un protocolo de aplicación para transferir recursos a través de Internet.

HTTP usa el Puerto 80, que es el puerto desde el que el servidor web acepta peticiones.

La mayoría de los recursos son archivos (imágenes, etc.) pero puede incluir otro tipo de datos como scripts.

Las sesiones HTTP se abren por un cliente HTTP (es decir, el navegador del usuario) a través de un agente de usuario y se envía un mensaje de petición de conexión al servidor HTTP (es decir, el servidor web). El mensaje de petición se conoce también como 'petición del cliente' y consiste en las siguientes líneas:

Línea de petición Encabezadps Línea vacía Un cuerpo del mensaje opcional Una vez que la respuesta ha sido entregada el servidor web cierra la conexión.

Este tipo de conexión es conocido como Stateless. La conexión solo existe por el periodo que

dure el intercambio de datos.

En función de la disponibilidad o no del recurso, HTTP proporciona un código de estatus apropiado (también conocido como 'respuesta del servidor'), determinado por el protocolo. Son los siguientes:

1xx: un simple mensaje informativo

2xx: éxito de algún tipo (ej: 200 OK - file found)

3xx: el cliente a otra URL (ej: 301 moved permanently)

4xx: un error en el lado del cliente (ej: 404 archivo no encontrado)

5xx: un error en el lado del servidor (ej: 500 server error)

DNS

El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space). Su labor primordial consiste en resolver las peticiones de asignación de nombres. Esta función se podría explicar mediante una comparación con un servicio telefónico de información que dispone de datos de contacto actuales y los facilita cuando alguien los solicita. Para ello, el sistema de nombres de dominio recurre a una red global de servidores DNS, que subdividen el espacio de nombres en zonas administradas de forma independiente las unas de las otras. Esto permite la gestión descentralizada de la información de los dominios.

Cada vez que un usuario registra un dominio, se crea una entrada WHOIS en el registro correspondiente y esta queda almacenada en el DNS como un "resource record". La base de datos de un servidor DNS se convierte, así, en la compilación de todos los registros de la zona del espacio de nombres de dominio que gestiona.

Cuando se quiere acceder a una página web en Internet se necesita la dirección IP del servidor donde está almacenada, pero, por regla general, el usuario solo conoce el nombre del dominio. La razón no es otra que la dificultad de recordar las series numéricas del tipo 93.184.216.34 que las componen, que son las que, precisamente, constituyen la base de la comunicación en Internet. Es por este motivo por el que las direcciones IP se "traducen" en nombres que podamos recordar, los llamados dominios:

Dirección IP: 93.184.216.34

Dominio:www.ejemplo.es

El proceso de traducción de los nombres de dominio en direcciones numéricas que las máquinas puedan entender es lo que se conoce como resolución de nombres, una labor que realiza el Domain Name System, en castellano Sistema de Nombres de Dominio, conocido por sus siglas DNS.

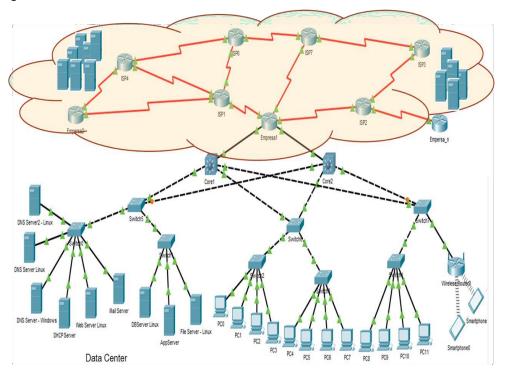
Herramientas a utilizar

- Computadores
- Acceso a Internet

Software de virtualización

Infraestructura base

Seguimos trabajando usando como guía la infraestructura de una organización como la presentada en el siguiete diagrama



En este laboratorio realizaremos configuraciones de nuevos servicios relacionadas con la plataforma base requerida para que una empresa mantenga conectividad. Dentro de los servidores se pueden encontrar servicios web, DNS, correo, Base de datos, almacenamiento y aplicaciones, entre otros. En esta oportunidad se configurará el servicio de DNS.

Experimentos

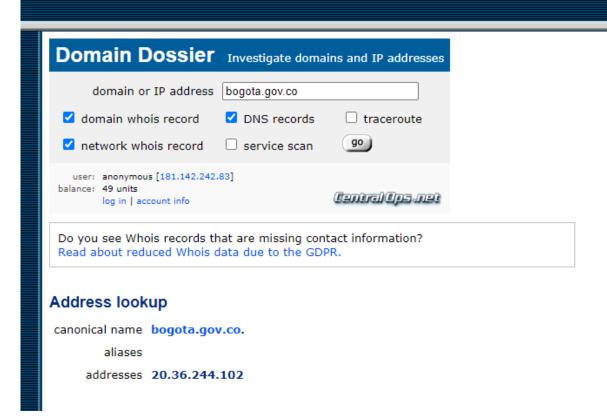
Realice las siguientes pruebas:

1. Prueba con equipos

- Ingrese a https://centralops.net/co/ y consulte los dominios
 - o bogota.gov.co
 - o presidencia.gov.co
 - o ejercito.mil.co
 - o Pruebe uno más que corresponda a una organización que sea de Estado Unidos.

Para cada uno de ellos presente los resultados obtenidos mediante un pantallazo y responda las siguientes preguntas (no todas las preguntas se pueden responder para todos los dominios, cree un cuadro con la información y si no aparecen los datos solicitados escriba NI - No contiene información):

Para bogota.gov.co:



Domain Whois record

```
Queried whois.nic.co with "bogota.gov.co"...
```

```
Domain Name: bogota.gov.co
Registry Domain ID: D604444-CO
Registrar WHOIS Server:
Registrar URL: www.cointernet.com.co
Updated Date: 2020-02-15T22:43:15Z
Creation Date: 1999-11-18T00:00:00Z
Registry Expiry Date: 2025-02-09723:59:592
Registrar: .CO Internet S.A.S.
Registrar IANA ID: 111111
Registrar Abuse Contact Email: soporte@cointernet.com.co
Registrar Abuse Contact Phone: +57.16169961
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: ALCALDIA MAYOR DE BOGOTA D. C.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: NA
Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: CO
 Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registran Registry Admin ID: REDACTED FOR PRIVACY
 Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
```

```
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Adm
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registran of Record identified in this output for information on how to contact the Registrant, Admi
Name Server: ns1-auth.etb.net.co
Name Server: ns2-auth.etb.net.co
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-12-02T23:14:38Z <<<
```

Network Whois record Queried whois.arin.net with "n 20.36.244.102"... 20.33.0.0 - 20.128.255.255 NetRange: 20.34.0.0/15, 20.48.0.0/12, 20.128.0.0/16, 20.64.0.0/10, 20.33.0.0/16, 20.40.0.0/13, 20.36.0.0/14 CIDR: NetName: MSFT NET-20-33-0-0-1 NET20 (NET-20-0-0-0) NetHandle: Parent: NetType: Direct Assignment OriginAS: Organization: Microsoft Corporation (MSFT) RegDate: 2017-10-18 Updated: 2017-10-18 https://rdap.arin.net/registry/ip/20.33.0.0 Ref: Microsoft Corporation OrgName: MSFT One Microsoft Way OrgId: Address: City: StateProv: Redmond WA PostalCode: 98052 Country: 1998-07-10 RegDate: Updated: 2017-01-28 To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malic Comment: Comment: * https://cert.microsoft.com. Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact: \star abuse@microsoft.com. Comment: Comment:

To report security vulnerabilities in Microsoft products and services, please contact: \star secure@microsoft.com.

For legal and law enforcement-related requests, please contact:

Comment:

Comment: Comment:

Comment: To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malic Comment: * https://cert.microsoft.com. Comment: Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact: Comment: abuse@microsoft.com. Comment: To report security vulnerabilities in Microsoft products and services, please contact: Comment: Comment: * secure@microsoft.com. Comment: Comment: For legal and law enforcement-related requests, please contact: * msndcc@microsoft.com Comment: Comment: For routing, peering or DNS issues, please Comment: Comment: contact:
* IOC@microsoft.com Comment: Ref: https://rdap.arin.net/registry/entity/MSFT OrgAbuseHandle: MAC74-ARIN OrgAbuseName: Microsoft Abuse Contact OrgAbusePhone: +1-425-882-8080 OrgAbuseEmail: abuse@microsoft.com https://rdap.arin.net/registry/entity/MAC74-ARIN OrgAbuseRef: OrgTechHandle: MRPD-ARIN OrgTechName: Microsoft Routing, Peering, and DNS OrgTechPhone: +1-425-882-8080 OrgTechEmail: IOC@microsoft.com https://rdap.arin.net/registry/entity/MRPD-ARIN OrgTechRef:

DNS records

DNS query for 102.244.36.20.in-addr.arpa returned an error from the server: NameError

| name | class | type | data | | time to live | | | | | |
|----------------------------|---|------|----------------|--|--------------|-----------|--|--|--|--|
| bogota.gov.co | IN | NS | ns2-auth.etb.n | net.co | 28800s | (08:00:00 | | | | |
| bogota.gov.co | IN | NS | ns1-auth.etb.n | ns1-auth.etb.net.co | | | | | | |
| bogota.gov.co | IN | TXT | google-site-ve | rification=fEjKN2X7AAbZ90ed-k0baIa6ykfByfrVuBrK6MHIKis | 3600s | (01:00:00 | | | | |
| bogota.gov.co | IN | Α | 20.36.244.102 | 20.36.244.102 | | | | | | |
| bogota.gov.co | IN | SOA | server: | ns1-auth.etb.net.co | 28800s | (08:00:00 | | | | |
| email: | | | | postmaster@etb.net.co | | | | | | |
| | | | serial: | 160 | | | | | | |
| refresh: | | | | 10800 | | | | | | |
| | | | retry: | 3600 | | | | | | |
| | | | expire: | | | | | | | |
| | | | minimum ttl: | 900 | | | | | | |
| end URL for this output | end URL for this output return to CentralOps.net, a service of Hexillion | | | | | | | | | |

| ¿Cuántos servidores de dominio tiene? | |
|--|------------------------------|
| ¿Hace cuánto fue asignado ese dominio? | 1999-Nov-18 |
| ¿Ante quién está registrado? | .CO Internet S.A.S. |
| ¿Cuál es el ID de la entidad de registro? | D604444-CO |
| ¿Cuándo fue actualizado el registro por última vez? | 2020-Feb-15 |
| ¿Hasta cuándo está activo dicho registro? | 2025-Feb-09 |
| ¿Cuál es el rango IP asignado y por cuál autoridad de registro fue dado? | 20.33.0.0 - 20.128.255.255 |
| ¿A cuál empresa le fue asignado? | Alcaldía mayor de Bogotá D.C |

Para presidencia.gov.co:

```
Domain Whois record
Queried whois.nic.co with "presidencia.gov.co"...
Domain Name: presidencia.gov.co
Registry Domain ID: D606208-CO
Registrar WHOIS Server:
Registrar URL: www.cointernet.com.co
Updated Date: 2020-11-08T14:48:10Z
Creation Date: 1999-10-29T00:00:00Z
Registry Expiry Date: 2025-11-02723:59:59Z
Registrar: .CO Internet S.A.S.
Registrar IANA ID: 111111
Registrar Abuse Contact Email: soporte@cointernet.com.co
Registrar Abuse Contact Phone: +57.16169961
 Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: DAFRE
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Bogota
Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: CO
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please guery the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR FRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
```

```
Admin Street: REDACTED FOR FRIVACY
Admin State/Frowince: REDACTED FOR FRIVACY
Admin For REDACTED FOR FRIVACY
Admin FAN REDACTED FOR FRIVACY
Tech Name REDACTED FOR FRIVACY
Tech Name REDACTED FOR FRIVACY
Tech State: REDACTED FOR FRIVACY
Tech FAN R
```

```
Network Whois record
Queried whois.lacnic.net with "190.145.219.29"...
               190.144.0.0/14
inetnum:
status:
               allocated
aut-num:
               N/A
owner:
                Telmex Colombia S.A.
ownerid:
               CO-ACSA-LACNIC
               CO-MCOM-MAGNIC
Operaciones Core IP
CLARO FIJO COLOMBIA - Cra 68A No. 24B-10, 11111,
11111 - Bogota - DC
responsible:
address:
address:
               CO
+57 01 7480000
country:
phone:
owner-c:
               ATI
abuse-c:
               ATI
                190.146.0.0/16
               NS3.TELMEXLA.NET.CO
nserver:
               20201201 AA
nslastaa:
               20201201
               NS2.TELMEXLA.NET.CO
20201201 AA
nsstat:
nslastaa:
               20201201
               190.147.0.0/16
NS3.TELMEXLA.NET.CO
inetrev:
               20201202 AA
nsstat:
               20201202
NS2.TELMEXLA.NET.CO
nslastaa:
nserver:
               20201202 AA
               20201202
190.144.0.0/16
NS3.TELMEXLA.NET.CO
nslastaa:
nserver:
               20201201 AA
nslastaa:
               20201201
               NS2.TELMEXLA.NET.CO
```

```
nslastaa:
                 20201201
nserver:
                NS2.TELMEXLA.NET.CO
                 20201201 AA
nsstat:
nslastaa:
inetrev:
                 190.145.0.0/16
                NS3.TELMEXLA.NET.CO
nserver:
                 20201126 AA
nsstat:
nslastaa:
nserver:
                NS2.TELMEXLA.NET.CO
                20201126 AA
nsstat:
                20201126
nslastaa:
created:
                20070111
changed:
                20070111
nic-hdl:
                ATI
person:
                Network Security Team
                abuse@telmexla.net.co
Carrera 68a #24b-10, 00, Plaza Claro
111321 - Bogota - DC
e-mail:
address:
address:
                CO
+57 017480456 [81966]
20020909
country:
phone:
created:
                20200605
changed:
\$ whois.lacnic.net accepts only direct match queries. \$ Types of queries are: POCs, ownerid, CIDR blocks, IP \$ and AS numbers.
```

DNS records

DNS query for 29.219.145.190.in-addr.arpa returned an error from the server: NameError

 ${\tt DNS \; query \; for \; 2.1.0.0.0.0.0.0.1.8.0.0.0.3.9.0.0.0.0.0.0.0.0.0.0.0.0.0.2.7.1.0.1.0.8.2.ip6. arpa \; returned \; an \; error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; server: \; Name Error \; from \; the \; Server: \; Name Error \; from \; the \; Server: \; Name Error \; from \; Name Error \; from$

| | | | | · · | | |
|--------------------|-------|------|----------------|------------------------------|--------|------------|
| name | class | type | data | | time t | to live |
| presidencia.gov.co | IN | SOA | server: | ariadne.presidencia.gov.co | 900s | (00:15:00) |
| | | | email: | admin@presidencia.gov.co | | |
| | | | serial: | 2020112720 | | |
| | | | refresh: | 1200 | | |
| | | | retry: | 600 | | |
| | | | expire: | 1209600 | | |
| | | | minimum ttl: | 301 | | |
| presidencia.gov.co | IN | NS | ariadne.presid | encia.gov.co | 0s | (00:00:00) |
| presidencia.gov.co | IN | NS | bdpalacio.pres | idencia.gov.co | 0s | (00:00:00) |
| presidencia.gov.co | IN | Α | 170.246.114.2 | 139 | 30s | (00:00:30) |
| presidencia.gov.co | IN | MX | preference: | 5 | 360s | (00:06:00) |
| | | | exchange: | oxpalacio.presidencia.gov.co | | |
| presidencia.gov.co | IN | MX | preference: | 10 | 360s | (00:06:00) |
| - | | | | nxpalacio.presidencia.gov.co | | |
| | | | a | passas-p. sassas-sas-ga-1160 | | |
| presidencia.gov.co | IN | MX | preference: | 5 | 360s | (00:06:00) |

| | | | exenange. mxparaero.presidencia.gov.co | | |
|--------------------|----|------|---|------|------------|
| presidencia.gov.co | IN | MX | preference: 5 exchange: zxpalacio.presidencia.qov.co | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | google-site-verification=i 0i2aHdLeifmJM7R TEivCuurblw YtEdhrHp51il0 | 360s | (00:06:00) |
| presidencia.gov.co | | TXT | globalsign-domain-verification=ynqUB_TdDIexM50K56_qt2QTD06Rk96h9QVlmsE_CG | | (00:06:00) |
| presidencia.gov.co | IN | TXT | v=spf1 mx ip4:190.145.219.51 ip4:190.145.219.52 ip4:170.246.114.213 include:spf.protection.outlook.com -all | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | cisco-ci-domain-verification=50f370706a12aaca6d1d02152128404936a7b128da5b6237a2b36ef5f5a37094 | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | FpO49es0QXYbffjSog/a7fy9YD4imQHWc0GeyHdY4J+WGGSFeXJgU0pkiuDiY72WyywVaLJ5S5j8qRfqXYgdoA== | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | MS=ms11844033 | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | globalsign-domain-verification=7z1ceOCd0zC1qUDe7MhUJImRomI_0q1WfDFei2aMCS | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | 76zprdseVsrN0unusdWbxZ4CWPijFTmoHn9zXNC3D0o= | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | MS=ms37011212 | 360s | (00:06:00) |
| presidencia.gov.co | IN | TXT | MS=ms33132372 | 360s | (00:06:00) |
| presidencia.gov.co | IN | AAAA | 2801:172::930:81:0:12 | 360s | (00:06:00) |
| presidencia.gov.co | IN | SRV | priority: 100 | 5s | (00:00:05) |
| | | | weight: 1 | | |
| | | | port: 5061 (5061) | | |
| | | | target: sipfed.online.lync.com.presidencia.gov.co | | |
| presidencia.gov.co | IN | SRV | priority: 0 | 5s | (00:00:05) |
| | | | weight: 0 | | |

| presidencia.gov.co IN | TXT | MS=ms33 | 3132372 | 360s | (00:06:00) |
|--|------|-----------|---|------|------------|
| presidencia.gov.co IN | AAAA | 2801:172 | ::930:81:0:12 | 360s | (00:06:00) |
| presidencia.gov.co IN | SRV | priority: | 100 | 5s | (00:00:05) |
| | | weight: | | | |
| | | port: | 5061 (5061) | | |
| | | target: | sipfed.online.lync.com.presidencia.gov.co | | |
| presidencia.gov.co IN | SRV | priority: | 0 | 5s | (00:00:05) |
| | | weight: | 0 | | |
| | | port: | 5061 (5061) | | |
| | | target: | sip.presidencia.gov.co.presidencia.gov.co | | |
| presidencia.gov.co IN | SRV | priority: | 0 | 5s | (00:00:05) |
| | | weight: | 0 | | |
| | | port: | HTTPS (443) | | |
| | | target: | sip.presidencia.gov.co.presidencia.gov.co | | |
| presidencia.gov.co IN | SRV | priority: | 100 | 5s | (00:00:05) |
| | | weight: | 1 | | |
| | | port: | HTTPS (443) | | |
| | | target: | sipdir.online.lync.com.presidencia.gov.co | | |
| end URL for this output return to C | | | | | |

| ¿Cuántos servidores de dominio tiene? | |
|---|---------------------|
| ¿Hace cuánto fue asignado ese dominio? | 1999-Oct-29 |
| ¿Ante quién está registrado? | .CO Internet S.A.S. |
| ¿Cuál es el ID de la entidad de registro? | D606208-CO |
| ¿Cuándo fue actualizado el registro por | 2020-Nov-08 |
| última vez? | |
| ¿Hasta cuándo está activo dicho registro? | 2025-Nov-02 |
| ¿Cuál es el rango IP asignado y por cuál | NI |
| autoridad de registro fue dado? | |
| ¿A cuál empresa le fue asignado? | DAPRE |

Para ejercito.mil.co:



```
Domain Whois record
Queried whois.nic.co with "ejercito.mil.co"...
Domain Name: ejercito.mil.co
Registry Domain ID: D615857-CO
Registrar WHOIS Server:
Registrar URL: www.cointernet.com.co
Updated Date: 2020-01-06T22:25:21Z
Treation Date: 1998-07-03T00:00:00Z
Registry Expiry Date: 2024-12-31723:59:59Z
Registrar: .CO Internet S.A.S.
Registrar IANA ID: 11111
Registrar Abuse Contact Email: soporte@cointernet.com.co
Registrar Abuse Contact Phone: +57.16169961
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Ejercito Nacional de Colombia
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Bogota
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CO
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
```

```
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Adm
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admi Name Server: ns2.telmexla.net.co
Name Server: ns3.telmexla.net.co
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-12-02T13:50:55Z <<<
```

Network Whois record

Queried whois.lacnic.net with "45.183.247.140"...

45.183.247.0/24 allocated N/A GRUPO LUMA SAS inetnum: status: aut-num: owner: ownerid: CO-GRLU-LACNIC responsible: Carlos Alberto Zuluaga address: Carrera 13 #113-55, 113-5, -110111 - BogotÃ; - CU address: CO +57 17458177 [0000] country: phone: owner-c:

ESP33 ESP33 tech-c: abuse-c: inetrev:

ESP33 45.183.247.0/24 NSO.LUMA.CLOUD 20201129 AA nsstat: 20201129 20201129 NS1.LUMA.CLOUD 20201129 AA nslastaa: nserver: nsstat: 20201129 20190910 nslastaa: created: changed: 20190910

nic-hdl:

ESP33 Carlos Zuluaga person:

Carlos Zuluaga carloszuluaga@lumacloud.co Carrera 13, 11355, -110111 - BogotĂ; - Cundinamarca CO +57 17458177 [0000] 20180430 20190715 e-mail: address:

address: country:

phone:

created:

changed:

\$ whois.lacnic.net accepts only direct match queries. \$ Types of queries are: POCs, ownerid, CIDR blocks, IP \$ and AS numbers.

DNS records

| Ditto records | | | | | |
|-----------------------------|-------|-------|---------------|--|---------------------|
| name | class | type | data | | time to live |
| ejercito.mil.co | IN | NS | ns3.telmexla. | net.co | 86400s (1.00:00:00) |
| ejercito.mil.co | IN | NS | ns2.telmexla. | net.co | 86400s (1.00:00:00) |
| ejercito.mil.co | IN | MX | preference: | 10 | 86400s (1.00:00:00) |
| | | | exchange: | correo.ejercito.mil.co | |
| ejercito.mil.co | IN | Α | 45.183.247.1 | 40 | 86400s (1.00:00:00) |
| ejercito.mil.co | IN | TXT | v=spf1 mx a | ip4:186.144.33.203 ip4:186.144.33.213 -all | 86400s (1.00:00:00) |
| ejercito.mil.co | IN | SOA | server: | ns3.telmexla.net.co | 86400s (1.00:00:00) |
| | | | email: | internet@telmexla.net.co | |
| | | | serial: | 2020042249 | |
| | | | refresh: | 1200 | |
| | | | retry: | 7200 | |
| | | | expire: | 1209600 | |
| | | | minimum ttl: | 86400 | |
| 140.247.183.45.in-addr.arpa | IN | PTR | 140.247.183. | 45.static.luma.cloud | 3600s (01:00:00) |
| 140 247 102 45 in-addrarna | TM | DDCTC | | | 2600c (01:00:00) |

| 140.247.183.45.in-addr.arpa | IN | PTR | 140.247.183. | 45.stati | c.luma.cloud | 3600s | (01:00:00) |
|------------------------------|------|-------|--------------------------|-----------|--|-----------|------------|
| 140.247.183.45.in-addr.arpa | IN | RRSIG | type covered | : | PTR (12) | 3600s | (01:00:00) |
| | | | algorithm: | | ECDSA Curve P-256 with SHA-256 (13) | | |
| | | | labels: | | 6 | | |
| | | | original ttl: | | 3600 (01:00:00) | | |
| | | | signature ex | piration: | 2020-12-10 00:00:00Z | | |
| | | | signature inc | eption: | 2020-11-19 00:00:00Z | | |
| | | | key tag: | | 20412 | | |
| | | | signer's nam | e: | 247.183.45.in-addr.arpa | | |
| | | | signature: (512 bits) | | 02F85D1FB8D17DEDEA407F10CA694FE5 D99241A7DF9DF4754648F2F4B35A2609 D54204DE44BD100FA81F8D01C87F6B8C 609F18AF4628914513CE787426803173 | | |
| 140.247.183.45.in-addr.arpa | IN | NSEC | next domain | name: | 141.247.183.45.in-addr.arpa | 3600s | (01:00:00) |
| | | | record types | | PTR RRSIG NSEC | | |
| 140.247.183.45.in-addr.arpa | TNI | RRSIG | | | | 3600e | (01:00:00) |
| 110.217.105.45.iii addi.arpa | 2114 | MOIG | type covered | : | NSEC (47) | 50003 | (01.00.00) |
| | | | algorithm: | | ECDSA Curve P-256 with SHA-256 (13) | | |
| | | | labels: | | 6 | | |
| | | | original ttl: | _! | 3600 (01:00:00) | | |
| | | | _ | | 2020-12-10 00:00:00Z | | |
| | | | signature inc | eption: | 2020-11-19 00:00:00Z | | |
| | | | | | | | |
| | | | signature incept | ion: 20 |)20-11-19 00:00:00Z | | |
| | | | key tag: | | 0412 | | |
| | | | signer's name: | 24 | 7.183.45.in-addr.arpa | | |
| | | | signature: (512 bits) | OC AF | F3A4DDDE3381B5DABFF7AFAAE87462 :26CCC022D9A1FB3D486D7EE58138C1 :EE95397D342714B1F01433069AE14D :82F8520D1AEC6BF8BC50BA75CCB23B | | |
| 247.183.45.in-addr.arpa IN | N | SOA | server: ns | s0.luma. | cloud 36 | 00s (01:0 | 0:00) |
| | | | email: he | ostmaste | er@247.183.45.in-addr.arpa | | |
| | | | serial: 1 | | | | |
| | | | refresh: 1 | 0800 | | | |
| | | | retry: 30 | 500 | | | |
| | | | expire: 1 | 209600 | | | |
| | | | minimum ttl: 3 | 500 | | | |
| 247.183.45.in-addr.arpa IN | N | RRSIG | type covered: | so | DA (6) 36 | 00s (01:0 | 0:00) |
| | | | 1 20 | | non o nose lil our ose (:-) | | |

algorithm: ECDSA Curve P-256 with SHA-256 (13)

original ttl: 3600 (01:00:00) signature expiration: 2020-12-10 00:00:00Z signature inception: 2020-11-19 00:00:00Z

signer's name: 247.183.45.in-addr.arpa

key tag: 20412

labels:

| | | | labels: | 5 | | |
|--------------------------|-----|-------|--------------------------|--|-------|------------|
| | | | original ttl: | 3600 (01:00:00) | | |
| | | | signature expiration: | 2020-12-10 00:00:00Z | | |
| | | | signature inception: | 2020-11-19 00:00:00Z | | |
| | | | key tag: | 20412 | | |
| | | | signer's name: | 247.183.45.in-addr.arpa | | |
| | | | signature: (512 bits) | DE1E9F3A1E13668C528671B5D03A803A 592A94D2BDCB23BB73FC3CD296E527DC 1E5C7DE33B3DC8626EC36376782397D3 C62D1A28DB152C410C7F7E4A9D6F562F | | |
| 247.183.45.in-addr.arpa | IN | NSEC | next domain name: | 0.247.183.45.in-addr.arpa | 3600s | (01:00:00) |
| | | | record types: | SOA RRSIG NSEC DNSKEY | | |
| 247.183.45.in-addr.arpa | IN | RRSIG | | | 2600e | (01:00:00) |
| 247.103.43.III-audi.aipa | IIV | KKSIG | type covered: | NSEC (47) | 30005 | (01.00.00) |
| | | | algorithm: | ECDSA Curve P-256 with SHA-256 (13) | | |
| | | | labels: | 5 | | |
| | | | original ttl: | 3600 (01:00:00) | | |
| | | | signature expiration: | 2020-12-10 00:00:00Z | | |
| | | | signature inception: | 2020-11-19 00:00:00Z | | |
| | | | key tag: | 20412 | | |
| | | | signer's name: | 247.183.45.in-addr.arpa | | |
| | | | signature: (512 bits) | 923D88AB0E752168487230325FFA0DF9 594D4B40D465896A10BC5D7ED84EB391 141C2B221FE870BCE282F0BF8D044BD0 | | |

| 247.183.45.m-addr.arpa | IIV | KKSIG | type covere | ed: | NSEC (47) | 30008 | (01:00:00) |
|-------------------------|-----|--------|---------------------------|----------------------|--|-------|------------|
| | | | algorithm: | | ECDSA Curve P-256 with SHA-256 (13) | | |
| | | | labels: | | 5 | | |
| | | | original ttl: | | 3600 (01:00:00) | | |
| | | | signature e | expiration: | 2020-12-10 00:00:00Z | | |
| | | | signature in | nception: | 2020-11-19 00:00:00Z | | |
| | | | key tag: | | 20412 | | |
| | | | signer's na | me: | 247.183.45.in-addr.arpa | | |
| | | | (512 bits) 5 | | 923D88AB0E752168487230325FFA0DF9 594D4B40D465896A10BC5D7ED84EB391 141C2B221FE870BCE282F0BF8D044BD0 D5587BBE509ECA406D971F5060BE68B5 | | |
| 247.183.45.in-addr.arpa | IN | DNSKEY | flags: | SecureEn | ntryPoint, ZoneKey (257) | 3600s | (01:00:00) |
| | | | protocol: | 3 | | | |
| | | | algorithm: | ECDSA C | urve P-256 with SHA-256 (13) | | |
| | | | public key: (512 bits) | 72D4E1A7 9D60EED4 | REAASCEF2297F4147D74DF597 RC697FAEA4969ABA09AB6A7A9 R2325D038170D718737C66859 R8F7EDDC2248E6F3663C9E3E5 | | |
| 247.183.45.in-addr.arpa | IN | RRSIG | type covere | ed: | DNSKEY (48) | 3600s | (01:00:00) |
| | | | algorithm: | | ECDSA Curve P-256 with SHA-256 (13) | | |
| | | | labels: | | 5 | | |
| | | | original ttl: | | 3600 (01:00:00) | | |
| | | | sianature e | expiration: | 2020-12-10 00:00:00Z | | |

594D4B40D465896A10BC5D7ED84EB391 (512 bits) 141C2B221FE870BCE282F0BF8D044BD0 D5587BBE509ECA406D971F5060BE68B5 247.183.45.in-addr.arpa IN DNSKEY 3600s (01:00:00) flags: SecureEntryPoint, ZoneKey (257) protocol: algorithm: ECDSA Curve P-256 with SHA-256 (13) public key: 4C8D8BD2EAA5CEF2297F4147D74DF597 72D4E1A7C697FAEA4969ABA09AB6A7A9 (512 bits) 9D60EED42325D038170D718737C66859 A6249D7E8F7EDDC2248E6F3663C9E3E5 247.183.45.in-addr.arpa RRSIG 3600s (01:00:00) type covered: DNSKEY (48) algorithm: ECDSA Curve P-256 with SHA-256 (13) labels: original ttl: 3600 (01:00:00) signature expiration: 2020-12-10 00:00:00Z signature inception: 2020-11-19 00:00:00Z key tag: 20412 signer's name: 247.183.45.in-addr.arpa signature: 023F80FD10C3583268855FE9388CBE78 9CF0B9CD4E57EA75D4A2953FD12CB55B (512 bits) EE6B832504852D5EFE555ED7FBC1DAF6 A76D00E497AF10CD83EDE526F859A7E7 -- end --URL for this output | return to CentralOps.net, a service of Hexillion

| ¿Cuántos servidores de dominio tiene? | | |
|---|-------------------------------|--|
| ¿Hace cuánto fue asignado ese dominio? | 1998-Jul-03 | |
| ¿Ante quién está registrado? | .CO Internet S.A.S. | |
| ¿Cuál es el ID de la entidad de registro? | D615857-CO | |
| ¿Cuándo fue actualizado el registro por | 2020-Ene-06 | |
| última vez? | | |
| ¿Hasta cuándo está activo dicho registro? | 2024-Dic-31 | |
| ¿Cuál es el rango IP asignado y por cuál | NI | |
| autoridad de registro fue dado? | | |
| ¿A cuál empresa le fue asignado? | Ejército Nacional de Colombia | |

Address lookup

canonical name adventuregamers.com.

aliases

addresses 104.26.7.138

172.67.74.151 104.26.6.138

2606:4700:20::681a:68a 2606:4700:20::ac43:4a97 2606:4700:20::681a:78a

Domain Whois record

Queried whois.internic.net with "dom adventuregamers.com"...

Domain Name: ADVENTUREGAMERS.COM
Registry Domain ID: 36086709_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.cloudflare.com
Registrar URL: http://www.cloudflare.com
Updated Date: 2018-12-10T05:15:582
Creation Date: 2000-09-25T18:28:002
Registry Expiry Date: 2024-09-25T18:28:00Z
Registrar: Cloudflare, Inc.
Registrar IANA ID: 1910
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DAN.NS.CLOUDFLARE.COM
Name Server: LADY.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation

DNSSEC DS Data: 2371 13 2 46124E2E067A4B4932E895B9A219BCB1BFA0A862ADC8D928E9DE3C7C875AFC08

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2020-12-03T23:43:55Z <<<

Network Whois record

Oueried whois.arin.net with "n 104.26.7.138"...

104.16.0.0 - 104.31.255.255 NetRange:

CIDR: 104.16.0.0/12 NetName: CLOUDFLARENET NET-104-16-0-0-1 NET104 (NET-104-0-0-0) NetHandle:

Parent:

NetType: Direct Assignment
OriginAS: AS13335
Organization: Cloudflare, Inc. (CLOUD14)
RegDate: 2014-03-28
Updated: 2017-02-17

All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse Comment:

https://rdap.arin.net/registry/ip/104.16.0.0 Ref:

OrgName: Cloudflare, Inc.

OrgId: CLOUD14

Address: 101 Townsend Street

San Francisco Citv:

StateProv: CA PostalCode: 94107 US Country:

2010-07-09 RegDate: 2019-09-25 Updated:

https://rdap.arin.net/registry/entity/CLOUD14 Ref:

OrgAbuseHandle: ABUSE2916-ARIN

OrgAbuseName: Abuse

OrgAbusePhone: +1-650-319-8930 OrgAbuseEmail: abuse@cloudflare.com

OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

OrgNOCHandle: NOC11962-ARIN

OrgNOCName: NOC

OrgNOCPhone: +1-650-319-8930 OrgNOCEmail: noc@cloudflare.com

OrgNOCRef: https://rdap.arin.net/registry/entity/NOC11962-ARIN

OrgTechHandle: ADMIN2521-ARIN

OrgTechName: Admin
OrgTechPhone: +1-650-319-8930 OrgTechEmail: rir@cloudflare.com

OrgTechRef: https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

RTechHandle: ADMIN2521-ARIN

RTechName: Admin RTechPhone: +1-650-319-8930

RTechEmail: rir@cloudflare.com RTechRef: https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

RAbuseHandle: ABUSE2916-ARIN

RAbuseName: Abuse

RAbusePhone: +1-650-319-8930 RAbuseEmail: abuse@cloudflare.com

https://rdap.arin.net/registry/entity/ABUSE2916-ARIN RAbuseRef:

RNOCHandle: NOC11962-ARIN

RNOCName: NOC

RNOCPhone: +1-650-319-8930 RNOCEmail: noc@cloudflare.com

RNOCRef: https://rdap.arin.net/registry/entity/NOC11962-ARIN

| DNS records | | | | | | |
|--|-------|-------|--------------------------|--|---------|-------------|
| name | class | type | data | | time to | live |
| adventuregamers.com | IN | Α | 104.26.7.138 | | 300s | (00:05:00) |
| adventuregamers.com | IN | Α | 172.67.74.151 | | 300s | (00:05:00) |
| adventuregamers.com | IN | Α | 104.26.6.138 | | 300s | (00:05:00) |
| adventuregamers.com | IN | RRSIG | type covered: | A (1) | 300s | (00:05:00) |
| | | | algorithm: | ECDSA Curve P-256 with SHA-256 (13) | | |
| | | | labels: | 2 | | |
| | | | original ttl: | 300 (00:05:00) | | |
| | | | signature expiration: | 2020-12-05 00:44:14Z | | |
| | | | signature inception: | | | |
| | | | key tag: | 34505 | | |
| | | | signer's name: | adventuregamers.com | | |
| | | | signature: (512 bits) | OD8CADF8C14DZEACFDD8SFEA29002BC0 88782B4B64BA67C875C9A56027A6AB9B 88065F4B19234216C074D91E81DD0AD1 189C9E50EB6FB89A920C24917A088D68 | | |
| adventuregamers.com | IN | NS | dan.ns.cloudflare.com | ı | 86400s | (1.00:00:00 |
| adventuregamers.com | IN | NS | lady.ns.cloudflare.com | 1 | 86400s | (1.00:00:00 |
| 138.7.26.104.in-addr.arpa | IN | HINFO | CPU: RFC8482 | | 3789s | (01:03:09) |
| | | | OS: | | | |
| 26.104.in-addr.arpa | IN | HINFO | CPU: RFC8482 | | 3789s | (01:03:09) |
| | | | OS: | | | |
| 26.104.in-addr.arpa | IN | NS | cruz.ns.cloudflare.com | n | 86400s | (1.00:00:00 |
| 26.104.in-addr.arpa | IN | NS | kevin.ns.cloudflare.co | m | 86400s | (1.00:00:00 |
| a.8.6.0.a.1.8.6.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.7.4.6.0.6.2.ip6.arpa | IN | HINFO | CPU: RFC8482 OS: | | 3789s | (01:03:09) |

| ¿Cuántos servidores de dominio tiene? | |
|---|-----------------------------|
| ¿Hace cuánto fue asignado ese dominio? | 2000-Sep-25 |
| ¿Ante quién está registrado? | Cloudflare, Inc. |
| ¿Cuál es el ID de la entidad de registro? | 36086709_DOMAIN_COM-VRSN |
| ¿Cuándo fue actualizado el registro por | 2020-May-14 |
| última vez? | |
| ¿Hasta cuándo está activo dicho registro? | 2024-Sep-25 |
| ¿Cuál es el rango IP asignado y por cuál | 104.16.0.0 - 104.31.255.255 |
| autoridad de registro fue dado? | |
| ¿A cuál empresa le fue asignado? | NI |

IN NS leah.ns.cloudflare.com

micah.ns.cloudflare.com

IN NS

73998s (20:33:18)

73998s (20:33:18)

• Uso del comando nslookup

0.0.7.4.6.0.6.2.ip6.arpa

0.0.7.4.6.0.6.2.ip6.arpa

- o ¿Para qué sirve el comando nslookup?
 - nslookup ejecuta un programa que es utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs.
- o Digite el comando ipconfig /all. ¿Quién es su servidor de DNS de su equipo?

```
Sufijo DNS específico para la conexión. . :
Descripción . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
Dirección física. . . . . . . . . . . . . . 6C-88-14-27-73-F4
DHCP habilitado . . . . . . . . . . . . . sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::a3:a3dd:aa12:7774%33(Preferido)
Dirección IPv4. . . . . . . . . . . : 192.168.1.2(Preferido)
Concesión obtenida. . . . . . . . . . : jueves, 3 de diciembre de 2020 1:43:31 p. m.
La concesión expira . . . . . . . . . . : viernes, 4 de diciembre de 2020 1:43:28 p. m.
Puerta de enlace predeterminada . . . . : 192.168.1.1
Servidor DHCP . . . . . . . . . . . . . . . . 192.168.1.1
IAID DHCPv6 . . . . . . . . . . . . . . . . . . 560760852
200.21.200.80
NetBIOS sobre TCP/IP. . . . . . . . : habilitado
```

Es un servidor con la dirección IP 200.21.200.10.

Corrobore el resultado digitando el comando ns lookup. ¿Quién es su servidor de DNS?.

```
C:\Users\lenovo>nslookup
Servidor predeterminado: dns4.telecom.com.co
Address: 200.21.200.10
```

Aguí se puede ver además de la dirección del DNS el dominio de este.

Se puede observar que es la dirección

- o Resolución de nombres
 - Digite el comando nslookup
 - En la línea de comandos de nslookup digite 2 nombres de servidores de la Escuela. Ej. www.escuelaing.edu.co. Documente el resultado obtenido y explíquelo.

```
Símbolo del sistema - nslookup
Microsoft Windows [Versión 10.0.19041.630]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Acer>nslookup
Servidor predeterminado: dnsbar.une.net.co
Address: 181.70.124.110
 www.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Respuesta no autoritativa:
Nombre: stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
Addresses: 3.213.223.141
         52.87.143.234
          52.21.175.83
         3.213.190.117
          52.206.15.164
          34.195.187.253
          54.175.121.11
          52.73.16.193
Aliases: www.escuelaing.edu.co
```

Después según lo que muestra la imagen el resultado son cada una de las direcciones que pertenecen al dominio de la escuela, es decir cada una de ellas identifica por asi decirlo al dominio, sale respuesta no autoritativa puesto que al hacer la consulta de este dominio nuestro computador no accedió directamente a ese dominio sino que tuvo que pasar por varios hasta llegar a este, también aparece el nombre del dominio que en este caso es "stark-chrimoya-jg28tzhyu4qth9c744i6vz0y.herokudns.com" y los alias que se tienen del dominio, con los cuales se puede acceder a este, aquí es donde se ubica lo que digitamos anteriormente www.escuelaing.edu.co

```
> www.campusvirtual.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110

Respuesta no autoritativa:
Nombre: www.campusvirtual.escuelaing.edu.co
Address: 149.56.16.159
>
```

Lo mismo pasa con la imagen anterior, la diferencia con la consulta de la anterior búsqueda de la escuela es que únicamente tiene una dirección que identifica a este dominio

 En la línea de comandos de nslookup digite 3 nombres de equipos fuera de la Escuela y que correspondan a diferentes dominios a nivel mundial ubicados en diferentes continentes.
 Documente el resultado obtenido y explíquelo.

Como se puede ver en las siguientes imágenes se consultaron dominios diferentes a los de la escuela, en cada uno de ellos esta una línea que dice "Respuesta no autoritativa" que lo que significa es que no se pudo llegar directamente al dominio que se deseaba llegar, sino que tuvo que pasar por varios dominios hasta llegar al que se quería.

También aparece el nombre del dominio que se deseo buscar y después el address o los addresses del dominio, en estos tres casos no fue como en el caso de la escuela donde habían varios address para el dominio de este, sino que cada uno de los dominios tenia únicamente un address.

Por ultimo aparece el alias o los alias del dominio por los cuales podemos acceder a ellos.

Símbolo del sistema - nslookup Microsoft Windows [Versión 10.0.19041.630] (c) 2020 Microsoft Corporation. Todos los derechos reservados. C:\Users\Acer>nslookup Servidor predeterminado: dnsbar.une.net.co Address: 181.70.124.110 > www.amazon.com Servidor: dnsbar.une.net.co Address: 181.70.124.110 Respuesta no autoritativa: Nombre: d3ag4hukkh62yn.cloudfront.net Address: 13.227.6.160 Aliases: www.amazon.com tp.47cf2c8c9-frontier.amazon.com > www.tesla.com.co Servidor: dnsbar.une.net.co Address: 181.70.124.110 Respuesta no autoritativa: Nombre: td-balancer-use1-24-83.wixdns.net Address: 34.73.24.83 Aliases: www.tesla.com.co www99.wixdns.net balancer.wixdns.net 55f818bb-balancer.wixdns.net

Respuesta no autoritativa:
Nombre: apple.com.co
Address: 17.253.142.4
Aliases: www.apple.com.co

> www.apple.com.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110

Respuesta no autoritativa:
Nombre: apple.com.co

o Cambie el servidor DNS que lo atiende al servidor DNS de la Escuela y realice las mismas consultas del punto anterior. Documente los resultados.

```
Símbolo del sistema - nslookup
Servidor predeterminado: UnKnown
Address: 45.239.88.68
> www.escuelaing.edu.co
Servidor: UnKnown
Address: 45.239.88.68
DNS request timed out.
   timeout was 2 seconds.
*** Se agotó el tiempo de espera de la solicitud a UnKnown
> www.apple.com.co
Servidor: UnKnown
Address: 45.239.88.68
DNS request timed out.
   timeout was 2 seconds.
*** Se agotó el tiempo de espera de la solicitud a UnKnown
```

Use el comando set type=NS y digite los mismos dominios el primer punto de esta sección.
 ¿Qué obtuvo? Muestre los resultados.

```
> set type=NS
```

```
Símbolo del sistema - nslookup
*** dnsbar.une.net.co no encuentra www.campusvirtual.escuelaing.edu.co/: Non-existent domain
> www.campusvirtual.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
campusvirtual.escuelaing.edu.co
        primary name server = ns10.dnsmadeeasy.com
        responsible mail addr = dns.dnsmadeeasy.com
        serial = 2009010113
        refresh = 43200 (12 hours)
        retry = 3600 (1 hour)
expire = 1209600 (14 days)
default TTL = 180 (3 mins)
> www.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Respuesta no autoritativa:
www.escuelaing.edu.co canonical name = stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
herokudns.com
        primary name server = dns1.p05.nsone.net
        responsible mail addr = hostmaster.nsone.net
        serial = 1607068035
        refresh = 600 (10 mins)
        retry = 900 (15 mins)
        expire = 1209600 (14 days)
        default TTL = 10 (10 secs)
```

Use el comando set debug y digite los mismos dominios el primer punto de esta sección.
 ¿Qué obtuvo? Muestre los resultados.

```
Símbolo del sistema - nslookup
 set debug
> www.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Got answer:
   HEADER:
        opcode = QUERY, id = 14, rcode = NOERROR
       header flags: response, want recursion, recursion avail.
        questions = 1, answers = 1, authority records = 1, additional = 0
    QUESTIONS:
       www.escuelaing.edu.co, type = NS, class = IN
    -> www.escuelaing.edu.co
        canonical name = stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
        ttl = 300 (5 mins)
    AUTHORITY RECORDS:
    -> herokudns.com
       ttl = 30 (30 secs)
        primary name server = dns1.p05.nsone.net
       responsible mail addr = hostmaster.nsone.net
        serial = 1607068140
       refresh = 600 (10 mins)
       retry = 900 (15 mins)
        expire = 1209600 (14 days)
       default TTL = 10 (10 secs)
```

```
Símbolo del sistema - nslookup
        default TTL = 10 (10 secs)
 www.campusvirtual.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Got answer:
    HEADER:
        opcode = QUERY, id = 15, rcode = NOERROR
       header flags: response, want recursion, recursion avail.
        questions = 1, answers = 0, authority records = 1, additional = 0
    OUESTIONS:
       www.campusvirtual.escuelaing.edu.co, type = NS, class = IN
    AUTHORITY RECORDS:
    -> campusvirtual.escuelaing.edu.co
       ttl = 180 (3 mins)
       primary name server = ns10.dnsmadeeasy.com
       responsible mail addr = dns.dnsmadeeasy.com
        serial = 2009010113
        refresh = 43200 (12 hours)
        retry = 3600 (1 hour)
        expire = 1209600 (14 days)
       default TTL = 180 (3 mins)
campusvirtual.escuelaing.edu.co
       ttl = 180 (3 mins)
       primary name server = ns10.dnsmadeeasy.com
       responsible mail addr = dns.dnsmadeeasy.com
```

```
campusvirtual.escuelaing.edu.co
ttl = 180 (3 mins)
primary name server = ns10.dnsmadeeasy.com
responsible mail addr = dns.dnsmadeeasy.com
serial = 2009010113
refresh = 43200 (12 hours)
retry = 3600 (1 hour)
expire = 1209600 (14 days)
default TTL = 180 (3 mins)
```

Use el comando set type=A y digite los mismos dominios el primer punto de esta sección.
 ¿Qué obtuvo? Muestre los resultados.

```
Símbolo del sistema - nslookup
> set type=A
> www.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Got answer:
   HEADER:
       opcode = QUERY, id = 16, rcode = NOERROR
       header flags: response, want recursion, recursion avail.
       questions = 1, answers = 9, authority records = 0, additional = 0
   QUESTIONS:
       www.escuelaing.edu.co, type = A, class = IN
    -> www.escuelaing.edu.co
       canonical name = stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       ttl = 105 (1 min 45 secs)
   -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 52.205.86.27
       ttl = 60 (1 min)
    -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 35.153.56.97
       ttl = 60 (1 min)
   -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 3.225.137.4
       ttl = 60 (1 min)
    -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 3.226.231.47
       ttl = 60 (1 min)
```

```
ttl = 60 (1 min)
   -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 54.221.249.251
       ttl = 60 (1 min)
   -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 3.222.114.249
       ttl = 60 (1 min)
   -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 52.55.160.36
       ttl = 60 (1 min)
   -> stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       internet address = 3.225.89.236
       ttl = 60 (1 min)
Respuesta no autoritativa:
Nombre: stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
Addresses: 52.205.86.27
         35.153.56.97
         3.225.137.4
         3.226.231.47
         54.221.249.251
         3.222.114.249
         52.55.160.36
         3.225.89.236
Aliases: www.escuelaing.edu.co
```

```
> www.campusvirtual.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Got answer:
   HEADER:
       opcode = QUERY, id = 17, rcode = NOERROR
       header flags: response, want recursion, recursion avail.
       questions = 1, answers = 1, authority records = 0, additional = 0
   OUESTIONS:
       www.campusvirtual.escuelaing.edu.co, type = A, class = IN
   -> www.campusvirtual.escuelaing.edu.co
       internet address = 149.56.16.159
       ttl = 1800 (30 mins)
Respuesta no autoritativa:
Nombre: www.campusvirtual.escuelaing.edu.co
Address: 149.56.16.159
```

 Use el comando set q=MX y digite los mismos dominios el primer punto de esta sección. ¿Qué obtuvo? Muestre los resultados.

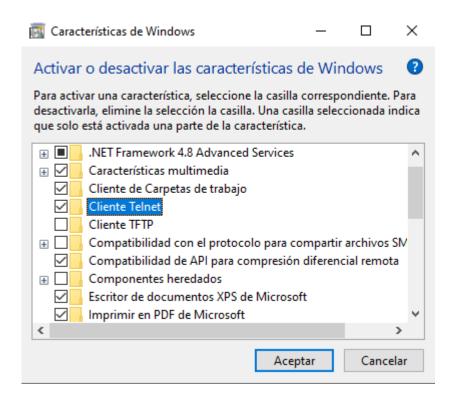
```
Símbolo del sistema - nslookup
 set q=MX
> www.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Got answer:
   HEADER:
       opcode = QUERY, id = 18, rcode = NOERROR
       header flags: response, want recursion, recursion avail.
       questions = 1, answers = 1, authority records = 1, additional = 0
   QUESTIONS:
       www.escuelaing.edu.co, type = MX, class = IN
   ANSWERS:
   -> www.escuelaing.edu.co
        canonical name = stark-cherimoya-jg38tzhyu4qth9c744i6vz0y.herokudns.com
       ttl = 300 (5 mins)
   AUTHORITY RECORDS:
    -> herokudns.com
       ttl = 30 (30 secs)
       primary name server = dns1.p05.nsone.net
       responsible mail addr = hostmaster.nsone.net
       serial = 1607068481
       refresh = 600 (10 mins)
       retry = 900 (15 mins)
       expire = 1209600 (14 days)
       default TTL = 10 (10 secs)
```

```
> www.campusvirtual.escuelaing.edu.co
Servidor: dnsbar.une.net.co
Address: 181.70.124.110
Got answer:
   HEADER:
        opcode = QUERY, id = 19, rcode = NOERROR
        header flags: response, want recursion, recursion avail.
        questions = 1, answers = 0, authority records = 1, additional = 0
        www.campusvirtual.escuelaing.edu.co, type = MX, class = IN
    AUTHORITY RECORDS:
    -> campusvirtual.escuelaing.edu.co
        ttl = 180 (3 mins)
        primary name server = ns10.dnsmadeeasy.com
        responsible mail addr = dns.dnsmadeeasy.com
        serial = 2009010113
        refresh = 43200 (12 hours)
        retry = 3600 (1 hour)
        expire = 1209600 (14 days)
        default TTL = 180 (3 mins)
campusvirtual.escuelaing.edu.co
        ttl = 180 (3 mins)
        primary name server = ns10.dnsmadeeasy.com
       responsible mail addr = dns.dnsmadeeasy.com
```

```
campusvirtual.escuelaing.edu.co
ttl = 180 (3 mins)
primary name server = ns10.dnsmadeeasy.com
responsible mail addr = dns.dnsmadeeasy.com
serial = 2009010113
refresh = 43200 (12 hours)
retry = 3600 (1 hour)
expire = 1209600 (14 days)
default TTL = 180 (3 mins)
```

2. Conexión HTTP

• Desbloquee el uso del protocolo TELNET en su computador.



• Realice captura de los paquetes de los protocolos TELNET y HTTP y muestre los mensajes de la capa de aplicación generados en las siguientes consultas:

- Capture la siguiente página web <u>http://profesores.is.escuelaing.edu.co/~csantiago/RECO/index.html</u> usando los protocolos así:
 - Telnet
 - Telnet profesores.is.escuelaing.edu.co 80
 - GET path/archivo. Ej GET /index.html. (No verá lo que escribe)



• Descargue el archivo tipo PDF prueba.pdf.

Descargue el archivo tipo imagen network.png.

```
Símbolo del sistema
                                                                                                                       "[&òU`ºþ®l*»£H§<sub>T</sub>ë«Õ¶U"[üØ£fF»E∎8uîµd»ICÕ∭kä¹≔-óØè
¡10_Õ¶[uÜQ$4ÍL«Ô<del>|0~=|></del>j`²FìnG⊖Ñ#
                                                                                                                                                                                                                                                                                                                                                       Jàμ"1Ö┐.~'§²dÒrÚî.♦0∰ÿqZÛêÉ)_Ö,∥-j4J
 üQ.3Ö4óÈ0∥õ∙ZúàrU¹³╓Ïdÿy└, Æ∥ʶFx®ÙÝ╨S´†Qmxs∰ÄLÅN§Ò)
    #É|iCBG9MBFÈᲡgqFÜxç#®÷BhrS6Ñ_BĬêl-h*_^dÖ@q99D.ወሷÓgäüJípùĭU<O-r#dVº]-၅:-½8Ĭ²ò┗ſ█*¤»、"%¡ ʰºᢤå¥Bj;ÈÚŒÑţOXV]Vo[wÁf·Am"Ngī]ªæk∰dÖUyJèµBB|-A|β#Bñ³³²¬ᆜ+tÒĀM>jp9q[ĒÉॐðº┱Ţ]
ŋtĒŷÝŗŶ.ŪÈB;ʔ;&k*OuTxrūÁŶ÷Ō zĀ-[¬Àhŋ∭e-R9Ō³z+÷o∞²m}OT_İ=ˈgt4Dæŋ∰däðiðSáj²ð∭bájákðgnáµB$¿Z-SÁuú muÉlWc%æiPUBā_խwáj_å{køð±"∯]8cX"å#ÄÄ |Æ-úTx:--iøuÒʿµქ8G«¾e=
Äqb}oUt#¢c█h'Íýo?Ü$ìB & V Br B e * ) M Vp 98 B cĪjS] B : W1 "î% <= Q C2 J KQM
wh6 W B ic K B J 'BR}4B nBP! u B h 8 58+ B
   ãOèô|é(¥ÊÁ·SÕÁé(Ê=ÑĐ|§\òQdË*Øf³B+R³ÇùJ»|ýsL"H
   D , © H iu l © i a{- [y b0 ~ 73> © P UW uj<! 'ihመZ Ç0 );U* ©p f R Hb2 ©`n
VyXu © © (b 5I!sh 4s%/ © Z y;- 8% j ~ Y©R j0 Uw +0 5 /HiE -u^m<
E K iy@ 3 Kz L|#[\N\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathrice{\mathric
 i≟Ùl<sub>■</sub>(」¹/{_q<sub>¶</sub> <mark>k</mark>À#∥Đ<sup>■</sup>ýuOò∭H(MA <sup>L</sup>áFò¬®I⊡üäv'¥÷Á»¢∥⊺)ıL┐ïÀ,¹Ø⊡D
                                                                                                                                                                                                                                                                                              Vô⊡#╨ë⊡»å¦w¶$r3«HÁ´╨ÕKÏZ™0â¹fþp´=,"GÓH─Ö>A¹ö¤
 98BA(ÜL
|Bµ0¶J$10-;ræ°À;+BKPE|¶Ý;8Á¬r[}Fā2~Z^©■Le|B|zXe?¢C■'B9?Mt)mā~Á§ìI2á~_;T¢■SUBXÌé§M<sup>U</sup>fÏvíhöLG[°JBV<sub>K</sub>L
B1ZBB"hirG
n»ex-¶ghàT<sup>U</sup>)X@+_≜xÍI{BOF¤/ÀZ«JLñYO$3µx^±ù@KBB6y²WÅåO=ç³æ;p-xON2°Bûµ<sup>UJ</sup>_*û¦WB³iv
                                                   ĭÂq'_N⊡V⊡ĭë=9üâ&∎ñ⊞i"lit⊞Ü&²È9Û¡<
ȿrú {- CK r T k⊡ jkk
 ZOBOBCT ~d>d %~
o h@BD & 4 T TJ1 B Y G mla 4J ? .d _ E f.Q Nt B 3P W tz D BO ,fXgI}j°zñ¥Ê}Áq"¡Z-|BUW_¿Ý=>äþ4∯£xYZ+ÖBafY>3ætÉfqú»â2H·Ø_U^ÿ¶.à_æ°cI²lqí
   /jóèË=9òOyêT¥<sup>L</sup>® ¶zÀxËk#lò^,$
"ıS<sub>1</sub>®á
                                                                                                      ÿ4߬kKJÙw"=Cd»E
                                                                                                                                                                    K;àGi40)(a5Ü£*%x5%Å7
È!zmVôj´y¤{|æ5ÜBÙ$tf®æð<mark>o</mark>BEEB@MA!`©J<mark>#</mark>a5\$O0|33s@¹Â;p-\E$|^BDĕTB?ðJ#Uz¹[ò+«pJ\jÂæevZx
|@ææ£?nñ}ôā=»B_{z«|]Ù9Bv±òx/!S\7B|zÑe§Z²HBJ±I+æâ:AJ^%=dIÕÆE´Gæ*~U£|ÑD|ÑÚŪJÀ>~oŌ;á<mark>+</mark>61%|q"+Úy∎%%#J
  ëil±÷+@.@_OÜe#lóãÄÑWlrä[]|Ù[´Ţ¡S@@@@yu@9Ä-{äÃtŋæÿXN$@Q¦;¬»küld@
```

• ¿Qué concluye?

HTTP

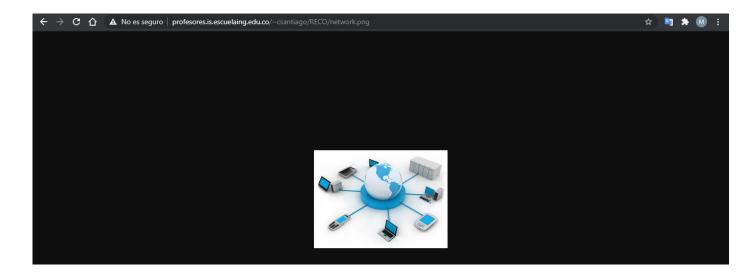
 Use el browser para mirar las mismas páginas que consultó a través de TELNET



Espacio de prueba del Laboratorio de RECO

Esta es un archivo de prueba para revisar el funcionamiento del protocolo HTTP y TCP





Instalación de software base

Como hemos visto en clase, otro servicios claves en un ambiente empresarial es el servicio Resolución de dominio - DNS. En este laboratorio vamos a configurar dicho servicio usando dos dominios de prueba.

Los dominios que se van a configurar son

- 1. estudiante1.com.co
- 2. estudiante2.edu.co
- 3. estudiante3.org.co

NOTA: reemplace "estudiante_n" por el apellido de los miembros del grupo. Ej: ardila.com.co

En cada dominio se deben definir

- 1. 3 servidores con sus equivalencias en IPv4 (Use las del rango que se les asignó al principio del semestre).
- 2. 2 servidores con sus equivalencias en IPv6 (Escoja las direcciones IPv6 que desee)
- 3. 2 alias para 2 servidor con dirección IPv4 y 1 servidor con dirección IPv6 (Seleccione los nombres que quiera ponerle)

La implementación debe realizarse usando dos máquinas virtuales, una Linux Centos y otra Linux Slackware y se debe instalar de la siguiente manera:

- Para el dominio estudiante1.com.co
 - Servidor DNS primario en una máguina virtual Centos
 - Servidor DNS secundario en una máguina virtual Slackware
- Para el dominio estudiante2.com.co
 - o Servidor DNS primario en una máquina virtual Slackware.
 - o Servidor DNS secundario en una máquina virtual Windows.
- Para el dominio estudiante3.com.co
 - Servidor DNS primario en una máquina virtual Windows.
 - Servidor DNS secundario en una máguina virtual Centos.

Use 3 máquinas virtuales en total para todo el grupo de 1,2 o 3 estudiantes: una Linux Slackware, otra Linux Centos y otra Windows Server. Para las pruebas de funcionamiento, cambie la configuración de DNS Cliente de las otras máquinas virtuales que ha configurado y haga pruebas de resolución de nombres.

1. Servidor DNS Primario Linux - BIND

A continuación, se presenta una guía para configurar el servicio de DNS primario.

a. Si lo requiere, instale el paquete de DNS del CD/Imagen de Linux

- b. Revise que los paquetes quedaron instalados (ej en el caso de Slackware use pkgtools para revisar).
- c. Configure el servicio

```
Servidor# vi /etc/named.conf
```

```
options {
  // Se define un directorio en donde se almacenará la información de los
  // dominios administrados. En este ejemplo se creó una carpeta DNS dentro de
  // de la carpeta /etc.
  directory "/etc/DNS";
  If there is a firewall between you and nameservers you want
  to talk to, you might need to uncomment the query-source
  directive below. Previous versions of BIND always asked
  questions using port 53, but BIND 8.1 uses an unprivileged
  port by default.
  */
  // query-source address * port 53;
// Zona para ir a los root server a resolver dominios no conocidos
zone "." IN {
     type hint;
     file "named.ca";
};
// Se crea una zona por cada dominio que se vaya a administrar. Se guarda la
   información en un archivo.
zone "mi_dominio" IN {
     type master;
     file "mi dominio.hosts";
     // Puede ser un nombre de archivo cualquiera, la recomendación es que le
        archivo se llame como se llama el dominio y use la extensión hosts pero
        podría llamares de cualquier forma. Ej. Archivo, datos.txt o abcdfg.xyz
      allow-update { none; };
// Para crear la zona reversa (segunda funcionalidad del servicio de DNS). Pero
// no la vamos a configurar ahora.
// zone "0.0.127.in-addr.arpa" IN {
```

```
//
      type master;
 //
      file "127.0.0.rev";
 //
         allow-update { none; };
 //};
Servidor# mkdir /etc/DNS
Servidor# vi /etc/DNS/named.ca 	❷ Busque en internet la lista e IPs de los ROOTSERVER. Solo
deje las equivalencia IPv4 (Puede borrarlas o ponerlas en comentarios)
          root name servers
          3600000
                           NS
                                 A.ROOT-SERVERS.NET.
                      ΙN
          root name servers by address
    // Buscar en internet la lista de root servers.
    A.ROOT-SERVERS.NET
                            3600000
                                       ΙN
                                             Α
                                                    abc.def.ghi.jkl
    ;A.ROOT-SERVERS.NET
                            3600000
                                       ΙN
                                             AAAA
                                                    2001:503:BA3E::2:30
    B.ROOT-SERVERS.NET
                            3600000
                                       ΙN
                                                    mno.pqr.stu.vwx
    C. ...
Servidor# vi /etc/DNS/mi_dominio.hosts 	✔ Cada estudiante deberá configurar su archivo.
       /etc/DNS/mi dominio.hosts file
          INCLUDE UPDATE SOA HEADER
                          ; puede incluirse o escribirse directamente la
    $INCLUDE named.soa
                          ; información aquí.
      Name Server(s)
    mi dominio.
                            NS
                                 esteServidor.mi dominio.
                                                             ;Pongale un nombre
                      ΙN
                                                              a esteServidor.
                                                              Ej. dns.mi dominio
      Mail Server(s)
    ; mi_dominio. MX
                                 10
                                       servidor_correo.mi_dominio.
    ; Address for localhost
    localhost.mi dominio.
                                             127.0.0.1
                               ΙN
    ; Addresses for the canonical names
    esteServidor.midominio.
                               IN A
                                        dir_IP_servidorDNS
                                        dir IP servidorHTTP
    nom real1.mi dominio.
                               IN A
```

```
nom_real2.mi_dominio.
                              IN A
                                         dir_IP_servidorXXXXX
    ; no se presenta la forma como se configura IPv6. Debe revisarse qué
    cambia.;
    ; Aliases
                             ΙN
                                               real1.mi dominio.
    alias1.mi dominio.
                                     CNAME
    alias2.mi_dominio.
                            IN
                                     CNAME
                                               real2.mi_dominio.
Servidor# vi /etc/DNS/named.soa 🕟 puede ser un archivo adicional o estar dentro de la zona
       /etc/DNS/named.soa file
      name server SOA file
                SOA
                      esteServidor.mi dominio.
                                                  root.mi dominio. (
    2020050101 ; serial
                   // El número usualmente es un consecutivo. El que el
                   // administrador desee usar, ej 001, 002, etc. En este
                   // ejemplo se usó aaaammddxx (aaaa: año, mm: mes,
                   // dd: día y xx: número consecutivo del día en el que
                   // se están haciendo las modificaciones).
                ; refresh
    43200
    3600
                ; retry
                ; expire
    432000
    86400
                ; minimum time-to-live
Servidor# /usr/sbin/named
```

d. ¿Qué son los registros A y AAAA en el archivo de rootserves?

Un registro A hace coincidencia de un dominio (o subdominio) con una dirección IP. En otras palabras, apunta su nombre de dominio a la dirección IP de su hosting, lo que permite que el tráfico web llegue a dicho servidor. Esta es la función principal del DNS. Un registro A típico luce así:

Registros A: Para direcciones IPv4 Registros AAAA: Para direcciones IPv6

```
ejemplo.com A 123.45.67.8
```

Un registro AAAA es lo mismo que un registro A, pero para direcciones IPv6. Un registro AAAA típico luce como el siguiente:

```
ejemplo.com AAAA 0123:4567:89ab:cdef:0123:4567:89ab:cdef
```

e. ¿Qué son los registros NS, MX, A y CNAME en el archivo de dominio particular?

Registro NS:

Los registros de Servidor de nombres (NS, del inglés "Name Server") determinan los servidores que comunicarán la información del DNS de un dominio. Por lo general, dispones de registros de servidor de nombres principales y secundarios para tu dominio. Cuando utilizas servicios de Google Cloud, puedes configurar

registros NS que señalen a los servidores de Google cuando se hagan consultas de DNS.

Registro MX:

específica donde los emails deberían ser entregados.

Registro A:

Específica las direcciones IP correspondientes a tus dominios y sub-dominios.

Registro CNAME:

Específica las redirecciones desde tus sub-dominios de los dominios a otros dominios/sub-dominios.

- f. Revise los logs del Sistema y use programa ns lookup para revisar que el servicio está funcionando bien.
- g. Pruebe su funcionamiento en un cliente
 - I. Configure un computador cliente para que use el servidor DNS que acaba de configurar.
 - II. Use wireshark para revisar los mensajes que circulan en la red cuando realice el procedimiento indicado en el ítem siguiente. Revise los mensajes de la capa de transporte y de la capa de aplicación.
 - III. Compruebe que el servicio funciona haciendo ping a las direcciones definidas en el servidor DNS. (Nota: el ping no necesariamente exitoso por no tener las máquinas operando o configuradas, pero la resolución de nombres funcionará).
- h. Pruebe su funcionamiento en el servidor DNS
 - I. Realice el paso anterior directamente en el servidor DNS, ¿funciona?, ¿por qué? ¿Qué es el resolv.conf?
 - II. Solucione el problema y muestre la configuración IP final del servidor
- i. Configure el servicio de resolución de dominios DNS de tal manera que se active durante el arranque del sistema.

Nota. La configuración de los servidores debe ser mostrada a su profesor.

Conclusiones

Durante este laboratorio se aprendió a entender y a practicar un poco con algunas aplicaciones y protocolos de la capa de aplicación como los son http,telnet,dns y asi mismo la forma de utilizar nuevos comandos como nslookup y la forma de configurar servidores DNS tanto primarios como secundarios. Se aprendió el uso de varias plataformas computacionales, tanto en Linux Slackware como en Windows Server.

<u>Bibliografia</u>

https://www.profesionalreview.com/2019/01/20/telnet-que-es/

https://www.pickaweb.es/ayuda/que-es-http/

https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-servidor-

dns-y-como-funciona/

https://culturacion.com/especial-modelo-osi-capa-de-

aplicacion/#:~:text=La%20capa%20de%20aplicaci%C3%B3n%20es,de%20bases%
20de%20datos%20y

http://campusvirtual.escuelaing.edu.co/moodle/mod/resource/view.php?id=15 1580

http://campusvirtual.escuelaing.edu.co/moodle/mod/resource/view.php?id=15 1577

http://campusvirtual.escuelaing.edu.co/moodle/mod/resource/view.php?id=15 1576

https://norfipc.com/redes/como-usar-comando-nslookup-

<u>windows.html#:~:text=1%2D%20Escribe%20en%20la%20consola,correo%20electr%C3%B3nico%20para%20el%20dominio.</u>

https://likegeeks.com/es/servidor-dns-de-linux/

https://www.redeszone.net/gnu-linux/configurar-un-servidor-dns-bind-en-linux-ubuntu/