

# Proyecto 1

## Criptografía

Emmanuel Peto Gutiérrez

7 de noviembre de 2020

### 1. whois

El comando `whois` en Linux sirve para mostrar toda la información sobre un dominio de internet.

Para este caso se buscó información del dominio de la secretaría de salud: `salud.gob.mx`.

```
emmanuel@emmanuel-VPCSB45FL:~$ whois salud.gob.mx

Domain Name:      salud.gob.mx
Created On:       2002-09-30
Expiration Date:  2021-09-29
Last Updated On:  2020-09-30
Registrar:       Akky (Una division de NIC Mexico)
URL:             http://www.akky.mx
Whois TCP URI:    whois.akky.mx
Whois Web URL:    http://www.akky.mx/jsf/whois/whois.jsf

Registrant:
  Name:           Direccion General de Tecnologias de la Informacion, Secretaria de Salud
  City:           Ciudad de Mexico
  State:          Ciudad de Mexico
  Country:        Mexico

Administrative Contact:
  Name:           Direccion General de Tecnologias de la Informacion, Secretaria de Salud
  City:           Ciudad de Mexico
  State:          Ciudad de Mexico
  Country:        Mexico

Technical Contact:
  Name:           Direccion General de Tecnologias de la Informacion, Secretaria de Salud
  City:           Ciudad de Mexico
  State:          Ciudad de Mexico
  Country:        Mexico

Billing Contact:
  Name:           Direccion General de Tecnologias de la Informacion, Secretaria de Salud
  City:           Ciudad de Mexico
  State:          Ciudad de Mexico
  Country:        Mexico

Name Servers:
  DNS:            itr.salud.gob.mx      187.210.186.246
```

## 2. nslookup

El comando `nslookup` se usa para encontrar la dirección IP de un dominio. También se puede usar para encontrar el dominio de una dirección IP.

Se buscó información del dominio `pemex.com`. La dirección IP se puede ver en internet address.

```
emmanuel@emmanuel-VPCSB45FL:~$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set debug
> pemex.com
Server:      8.8.8.8
Address:     8.8.8.8#53

-----
QUESTIONS:
  pemex.com, type = A, class = IN
ANSWERS:
-> pemex.com
  internet address = 200.188.13.39
  ttl = 59
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Non-authoritative answer:
Name:   pemex.com
Address: 200.188.13.39
-----
QUESTIONS:
  pemex.com, type = AAAA, class = IN
ANSWERS:
AUTHORITY RECORDS:
-> pemex.com
  origin = ddi-ext-mex.pemex.com
  mail addr = sitemaster.pemex.com
  serial = 2018081965
  refresh = 10800
  retry = 3600
  expire = 1209600
  minimum = 1200
  ttl = 4
ADDITIONAL RECORDS:
-----
> 
```

## 3. traceroute

El comando `traceroute` determina la ruta tomada desde mi computadora hasta un host en el internet. Se muestran los routers por los que pasa un paquete antes de llegar a su destino. También se muestra el tiempo que tarda en pasar de un punto a otro.

Se buscó la dirección IP de `unam.mx` con `lookup`. Uno de los resultados es `132.248.166.20`.

Se realizó un trazado de ruta hacia la dirección IP de la UNAM.

```
emmanuel@emmanuel-VPCSB45FL:~$ traceroute --resolve-hostnames 132.248.166.20
traceroute to 132.248.166.20 (132.248.166.20), 64 hops max
 1  192.168.1.254 (_gateway)  2.148ms  2.109ms  1.966ms
 2  201.154.0.76 (ipdsl-mex-popocatepetl-71-l0.uninet.net.mx)  7.310ms  11.210ms  11.183ms
 3  189.246.101.17 (itcam-nvl-triara-41-tge0-3-0-4.uninet.net.mx)  25.881ms  25.243ms  29.351ms
 4  189.247.253.14 (ext-189-247-253-14.uninet.net.mx)  23.155ms  25.061ms  20.364ms
 5  189.202.244.141 (141.189-202-244.bestelclientes.com.mx)  21.229ms  26.898ms  29.014ms
 6  201.148.69.177 (177.201-148-69.bestelclientes.com.mx)  112.035ms  21.442ms  21.484ms
 7  192.100.200.81 (192.100.200.81)  39.786ms  33.654ms  24.480ms
 8  132.247.237.221 (1006-timas.redunam.unam.mx)  90.862ms  97.282ms  92.334ms
 9  132.248.166.20 (132.248.166.20)  62.329ms !*  62.254ms !*  58.973ms !*
```

## 4. nmap

Nmap es una herramienta que se usa para determinar los hosts que se están ejecutando y los servicios que estos están ejecutando.

### 4.1. Escaneo de puertos TCP

```
emmanuel@emmanuel-VPCSB45FL:~$ nmap localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-06 23:25 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
631/tcp   open  ipp
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
emmanuel@emmanuel-VPCSB45FL:~$
```

## 4.2. Sistema operativo

```
emmanuel@emmanuel-VPCSB45FL: ~  
otocolNew, FoundRows, SupportsCompression, InteractiveClient, Supports  
MultipleStatements, SupportsAuthPlugins, SupportsMultipleResults  
| Status: Autocommit  
| Salt: %uLet0=Ya1eBC \x7F@.\x01=!  
|_ Auth Plugin Name: caching_sha2_password  
| ssl-cert: Subject: commonName=MySQL_Server_5.7.28_Auto_Generated_Ser  
ver_Certificate  
| Not valid before: 2019-11-26T23:48:29  
|_Not valid after: 2029-11-23T23:48:29  
5432/tcp open  postgresql PostgreSQL DB 9.5.11 - 9.5.16  
| ssl-cert: Subject: commonName=ubuntu  
| Not valid before: 2017-03-31T10:07:21  
|_Not valid after: 2027-03-29T10:07:21  
| ssl-date: TLS randomness does not represent time  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at ht  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds  
emmanuel@emmanuel-VPCSB45FL:~$
```