

Práctica 4

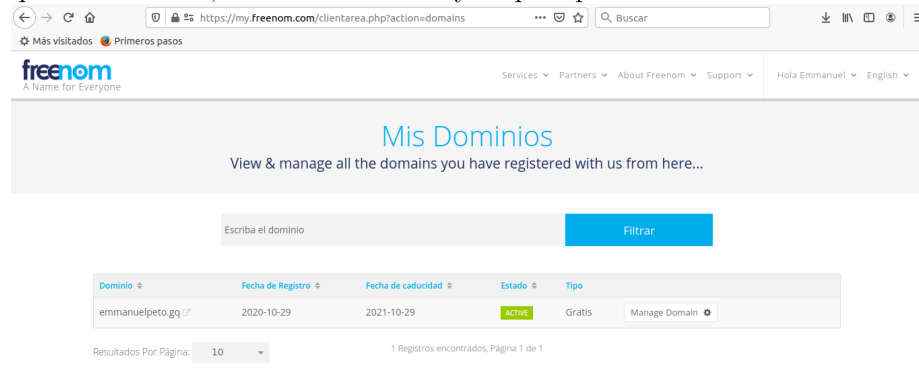
Redes de computadoras

Emmanuel Peto Gutiérrez

30 de octubre de 2020

1. Pasos para realizar la práctica

Se registró el dominio *emmanuelpeto.gq* en la página <https://www.freenom.com>. Para ello se colocó el nombre *emmanuelpeto* en el inicio de la página y se le dio click al botón azul que dice *Comprobar disponibilidad*. En la siguiente página se eligió la extensión *gq* y se dio finalizar compra. El tiempo por el que se eligió el dominio fueron 12 meses (que todavía es gratis). Finalmente se eligió iniciar sesión con Google, con la cuenta de ciencias. Se envió un enlace a mi correo para comprobar la cuenta, llené un formulario y después pude acceder.



En la sección de *Mis dominios* le di click al botón *Gestionar dominio*. Luego le di click en la pestaña *Gestionar DNS Freenom*. En esta página se elige el tipo A (que es para IPv4) y en *Target* se coloca la dirección IP elástica creada en la práctica 3.

DNS MANAGEMENT for emmanuelpeto.gq

[Back to domain details](#)

No records to display.

Add Records

Name	Type	TTL	Target
	A	3600	54.166.88.197

[+ More Records](#)

[Save Changes](#)

Si todo salió bien debería decir *Record added successfully*. Después de un tiempo se debería poder acceder a la página creada en la práctica 3 mediante el nombre de dominio.

[←](#) [→](#) [↺](#) [🏠](#) [🔒](#) [emmanuelpeto.gq](#)

[⚙️ Más visitados](#) [🌐 Primeros pasos](#)

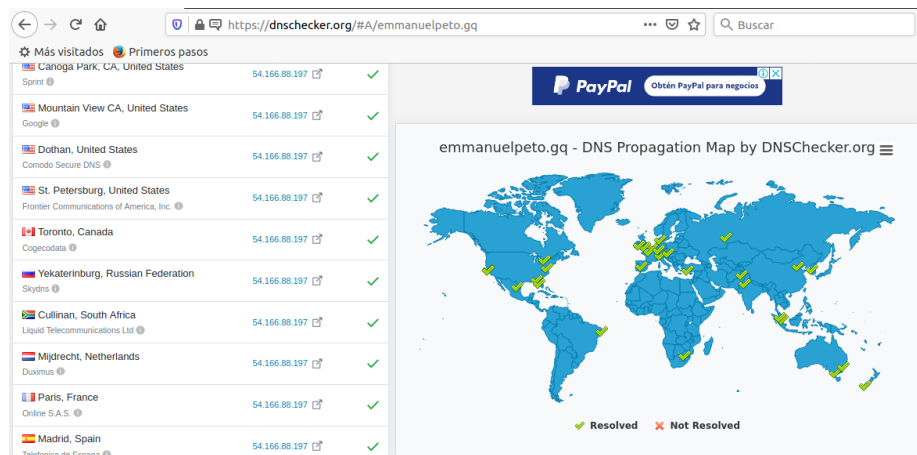
[Iniciar sesión](#)

User:

Pass:



Para revisar la propagación del nombre de dominio se usó la página dnschecker.org. Después de 16 horas (más o menos) de haber registrado el nombre de dominio se puede notar que ya se resolvió en todos los servidores DNS que se muestran en la página [dnschecker](https://dnschecker.org).

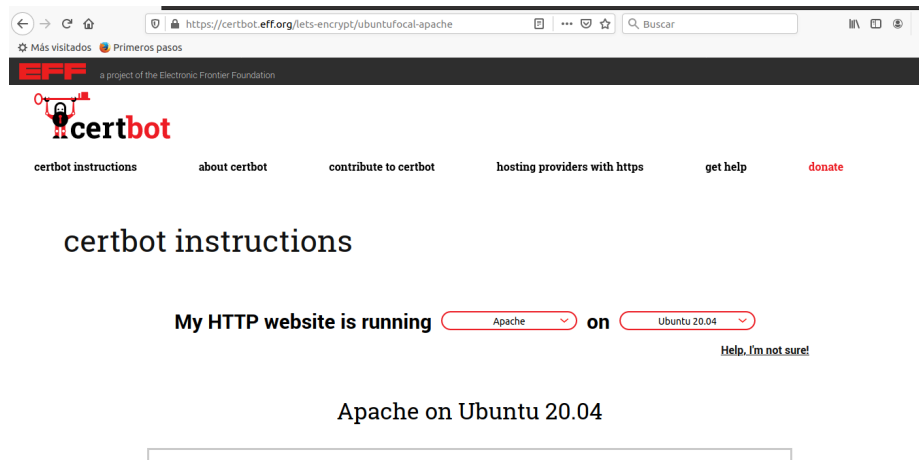


El siguiente paso es instalar un certificado de seguridad para el dominio que se acaba de crear. Para ello hay que ver el manual en la página letsencrypt.org. Hay que pinchar el botón *Empezar* de la página principal.

Para instalar el certificado hay que leer las instrucciones que dicen *Con acceso Shell*, ya que nosotros nos conectamos al servidor mediante SSH. Hay que hacer click en el enlace que dice *Certbot*.

El enlace nos lleva a la página de Certbot. En esta página hay una sección que dice *My website is running on - on -*, y hay que elegir el servidor Apache y el sistema operativo Ubuntu 20.04, que es el que se instaló en el servidor de AWS.

Una vez elegido el servidor y el sistema operativo se mostrarán las instrucciones para instalar el certificado.



1.1. Certbot

1. El primer paso es conectarse con el servidor mediante SSH, como ya se ha mostrado en las prácticas 2 y 3.
2. Se comprueba que se tenga instalado Snap con los comandos `sudo snap install core`; `sudo snap refresh core`.
3. Desinstalar paquetes Certbot que ya estén instalados en el sistema operativo (si es que lo están). Para esto se usa el comando `sudo apt-get remove certbot`. En mi caso, no había paquetes certbot instalados previamente.
4. Después, hay que instalar certbot con el comando `sudo snap install --classic certbot`.
5. Para garantizar que se puede ejecutar el comando certbot, ejecutar el siguiente comando: `sudo ln -s /snap/bin/certbot /usr/bin/certbot`.
6. Desconectarse del SSH y volverse a conectar pero ahora cambiando la dirección IP por el nombre de dominio. En mi caso:
`ssh -i 'practica2.pem' ubuntu@emmanuelpeto.gq`.
7. Ejecutar el siguiente comando para obtener un certificado y que Certbot edite la configuración de Apache automáticamente, encendiendo el acceso a HTTPS en un solo paso: `sudo certbot --apache`.

```
ubuntu@ip-172-31-81-18: ~
To see these additional updates run: apt list --upgradable

Last login: Wed Oct 21 23:26:10 2020 from 187.190.113.164
ubuntu@ip-172-31-81-18:~$ sudo snap install core; sudo snap refresh core
snap "core" is already installed, see 'snap help refresh'
snap "core" has no updates available
ubuntu@ip-172-31-81-18:~$ sudo apt-get remove certbot
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'certbot' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 37 not upgraded.
ubuntu@ip-172-31-81-18:~$ sudo snap install --classic certbot
certbot 1.9.0 from Certbot Project (certbot-eff) installed
ubuntu@ip-172-31-81-18:~$ sudo ln -s /snap/bin/certbot /usr/bin/certbot
ubuntu@ip-172-31-81-18:~$ sudo certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): empg014@ciencias.unam.mx

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.0-Nov-15-2016.pdf

-----
Congratulations! You have successfully enabled https://emmanuelpeto.gq
-----
Subscribe to the EFF mailing list (email: empg014@ciencias.unam.mx).

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/emmanuelpeto.gq/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/emmanuelpeto.gq/privkey.pem
  Your cert will expire on 2021-01-27. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot again
  with the "certonly" option. To non-interactively renew *all* of
  your certificates, run "certbot renew"
- Your account credentials have been saved in your Certbot
  configuration directory at /etc/letsencrypt. You should make a
  secure backup of this folder now. This configuration directory will
  also contain certificates and private keys obtained by Certbot so
  making regular backups of this folder is ideal.
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

ubuntu@ip-172-31-81-18:~$
```

Se puede comprobar la renovación automática de los certificados ejecutando el comando: `sudo certbot renew --dry-run`.

Nota: para poder conectarse mediante HTTPS hay que habilitarlo en el Security Group de AWS. Para esto hay que ir a EC2, buscar en el menú de la izquierda **Redes y seguridad/Security Groups**, dar click en el grupo de seguridad que se esté usando, dar click en **Editar reglas**, **Agregar regla**, elegir **HTTPS** y guardar.

← → ↻ 🏠 🔒 https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#SecurityGroups:sg-0c4cb6ecd5d62348

Más visitados Primeros pasos

aws Servicios

elastic block store

Volumenes

Instantáneas

Administrador del ciclo de vida

▼ Red y seguridad

Security Groups *New*

Direcciones IP elásticas *New*

Grupos de ubicación *New*

Pares de claves *New*

Interfaces de red

▼ Equilibrio de carga

Balancedadores de carga

Grupos de destino *New*

▼ Auto Scaling

Configuraciones de lanzamiento

Nombre del grupo de seguridad: launch-wizard-1

ID del grupo de seguridad: sg-0c4cb6ecd5d62348

Descripción: launch-wizard-1 created 2020-10-15T16:26:21.177-05:00

ID de la VPC: vpc-3c30f341

Propietario: 410863253565

Número de reglas de entrada: 4 Entradas de permisos

Número de reglas de salida: 1 Entrada de permiso

Reglas de entrada Reglas de salida Etiquetas

Reglas de entrada Editar reglas de entrada

Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional
HTTP	TCP	80	0.0.0.0/0	-
HTTP	TCP	80	:::0	-
SSH	TCP	22	0.0.0.0/0	-
HTTPS	TCP	443	0.0.0.0/0	-

Y ahora sí, ya se puede entrar a la página mediante https.

← → ↻ 🏠 🔒 https://emmanuelpeto.gq

Más visitados Primeros pasos

Iniciar sesión

User:

Pass:

enviar



Se envió información en el formulario con los valores: usuario → valentin, contraseña → elizalde.

No.	Time	Source	Destination	Protocol	Length	Info
98	39.967671404	192.168.1.42	54.166.88.197	TLSv1..	583	Client Hello
100	40.068960196	54.166.88.197	192.168.1.42	TLSv1..	1514	Server Hello, Change Cipher Spec, Application Data
102	40.069802144	54.166.88.197	192.168.1.42	TLSv1..	1514	Application Data [TCP segment of a reassembled PDU]
104	40.069857117	54.166.88.197	192.168.1.42	TLSv1..	279	Application Data, Application Data
106	40.072927094	192.168.1.42	54.166.88.197	TLSv1..	130	Change Cipher Spec, Application Data
107	40.073261315	192.168.1.42	54.166.88.197	TLSv1..	628	Application Data
109	40.174820461	54.166.88.197	192.168.1.42	TLSv1..	145	Application Data
111	40.175934536	54.166.88.197	192.168.1.42	TLSv1..	145	Application Data
114	40.231764947	54.166.88.197	192.168.1.42	TLSv1..	325	Application Data
138	45.245257265	54.166.88.197	192.168.1.42	TLSv1..	90	Application Data
141	45.245576315	192.168.1.42	54.166.88.197	TLSv1..	90	Application Data

Figura 1: Captura con GET.

Con el método GET se realiza la siguiente captura de tráfico. El protocolo usado para transmitir la información es Transport Layer Security (TLS). Notamos que en la sección *Application Data* hay texto cifrado.

La captura con el método POST es similar a la del método GET. También se muestra texto cifrado.

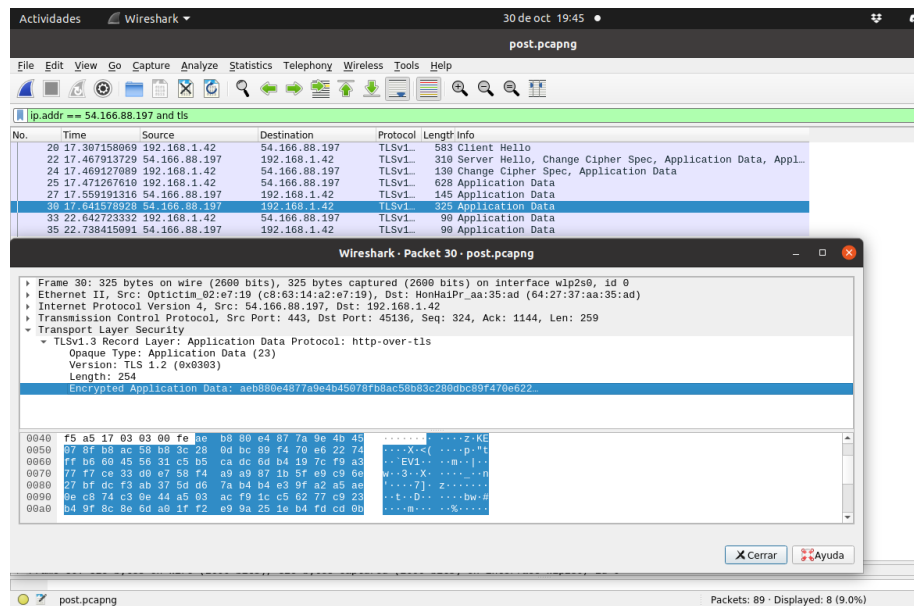


Figura 2: Captura con POST.

2. Cuestionario

1. ¿Qué es un DNS?

Es un sistema distribuido que sirve para traducir un nombre de dominio a una dirección IP.

2. ¿Qué es un registro A y qué elementos fueron necesarios para registrarlo en el DNS de Freenom?

Indica que el tipo de registro es de IPv4; es decir, se relaciona un nombre de dominio (`emmanuelpeto.gq`) con una dirección IPv4 (`54.166.88.197`).

Para registrarlo en Freenom, primero se verificó que estuviera disponible el nombre del dominio. Después se eligió la terminación `gq` porque era gratuito. Luego, en la sección *Gestionar dominio*, en la pestaña *Gestionar DNS Freenom* se eligió el tipo A y en *Target* se colocó la IP de la instancia creada en AWS.

3. ¿Qué es un registro CNAME y Cuál es la diferencia con el registro A?

Es el nombre canónico de un registro DNS, el cual asigna un alias a un nombre de dominio auténtico.

El registro A guarda la dirección IP de un dominio, mientras que el CNAME guarda un nombre alternativo para el dominio.

4. ¿Qué es HTTPS? y ¿Por qué es importante para tu seguridad?

Se utiliza para la transferencia de datos en la capa de aplicación, igual que el protocolo HTTP, pero éste lo hace cifrando los datos.

Es importante porque los usuarios realizamos transferencias bancarias, inicio de sesión, comunicación de datos personales, entre otras cosas, mediante el internet. Si los datos están cifrados no podrán ser interpretados por intrusos en la red hasta que llegen a su destino.

5. URL creada en la práctica

`https://emmanuelpeto.gq/`

6. Pantalla de tráfico seguro capturado con wireshark de tu formulario (usar metodo post)

- Método get: 1
- Método post: 2