Setting up a trusted Command and Control Server (C2 / C&C)

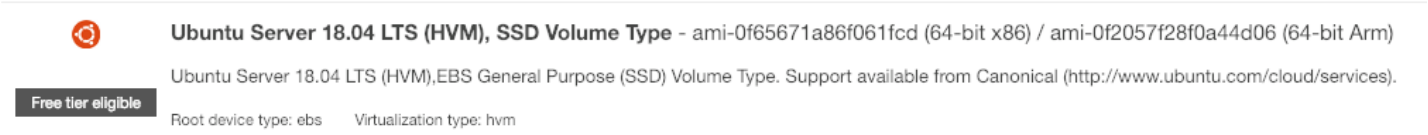
Author: Emilio Revelo
jose@emiliorevelo.com

Introduction

This paper covers one way to create a simple command and control server with a trusted certificate emited by a free CA, using Empire with that certificate to encrypt all the data trasmited between agents and listener.
hh
This can be very useful for all of those who wants to perform red team activities with a limited budget.

Initialize an Instance

There are many options (even free) that we could use to create a virtual server with a static public IP, in this case I used EC2 from AWS (I decided to use my 1 year of free tier).



In this example I used Ubuntu Server with apache2, then we just install it and start it:

```
# apt-get install apache2

# service apache2 start
```

```
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Fri 2019-01-18 18:30:18 UTC;
```

Then we just go to Instances/Description and check the public IP address.

Getting a Domain Name and link with your public IP

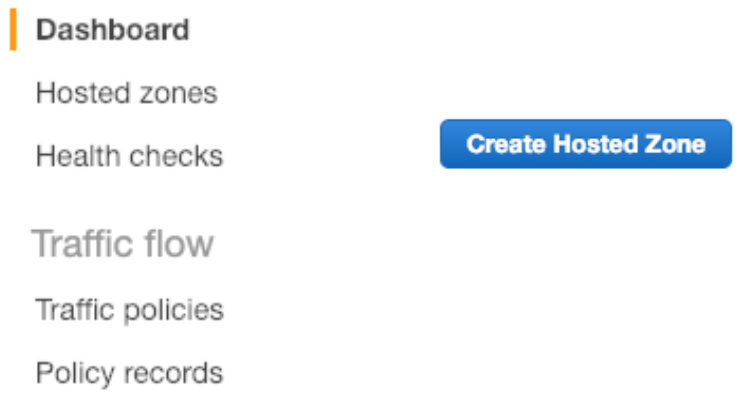
We going to use Let's encrypt that is a free, automated, and open Certificate Authority, but only can be used with domain names not with raw IP address.

There are many providers that sell cheap domain names, for example:

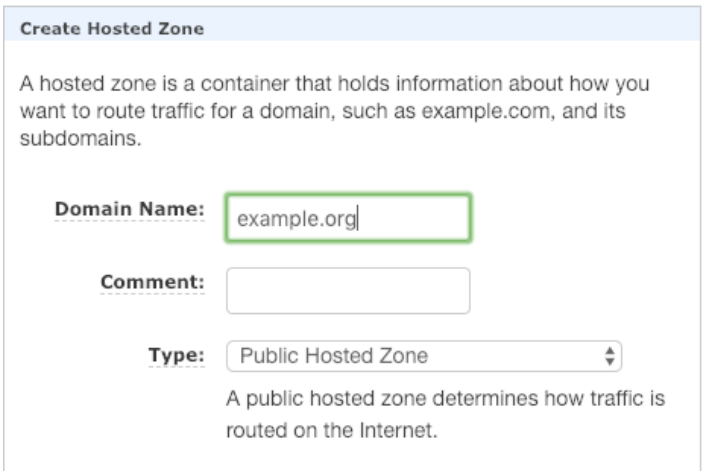
- Godday
- 1&1 (Actually IONOS)
- Namecheap
- Register
- Moniker
- etc…

Assuming that you already have a domain name with the provider that you prefer, then we go to our AWS console and do the follow to link our domain name with our EC2 IP:

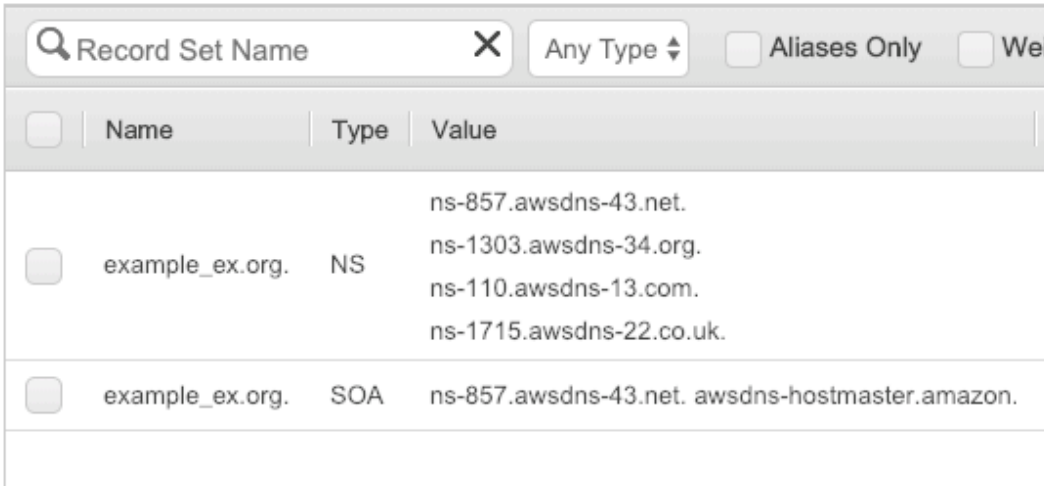
1- Go to **Route 53** option, select **Hosted Zones** and **Create Hosted Zone:**



Once there, in the right column you need to specify your domain name and click on create button.



After that, we then get the name servers that we going to use to redirect our site.



Finally we must select the option Create a Record Set to specify the IP address that will be linked with our domain name.

2- Whit your NS created, you must configure them in your domain name provider`s console. After a couple of minutes or hours this change will be applied.

Emiting a trusted certificate by a CA

We could use Let's Encrypt to create our trusted certificate, first we need to install certbot[1] by selecting Apache as a web server (or whichever you want) and the system OS, once that we have selected that options, we could see the instructions to install certbot (This is quite easy).

It's important to mention that Let's Encrypt[2] only issues certificates related to domain names, not for raw IP address, that's the reason why we must already have a domain name.

[1] https://certbot.eff.org/
[2] https://letsencrypt.org/

Setting up Empire with the previous certificate

Once that your trusted certificate is done, you must copy the next two files (To another path) located in ***/etc/letsencrypt*** and change their names as follows:

privkey1.pem -> **empire-priv.key**
fullchain1.pem -> **empire-chain.pem**

We must setting up an HTTPS with the next parameters:

Host: https://[domain name or IP]:Port
Port: 8080, 443, 80, etc…
CertPath: Path where you copied certificate´s files above.

And then execute the listener and start to connect clients.

References:

[1] https://certbot.eff.org/

[2] https://www.powershellempire.com/

[3] https://letsencrypt.org/