

Informe despliegue de app en la nube

Realizado por: *Luna Cantero Ángel Iván*
Martínez Ramírez Guadalupe Monserrat
Reyes Morales Salvador
Salazar León María Guadalupe

Cliente: *UTNG*

Fecha: *16/08/2023*

Organización: *EventickNow*

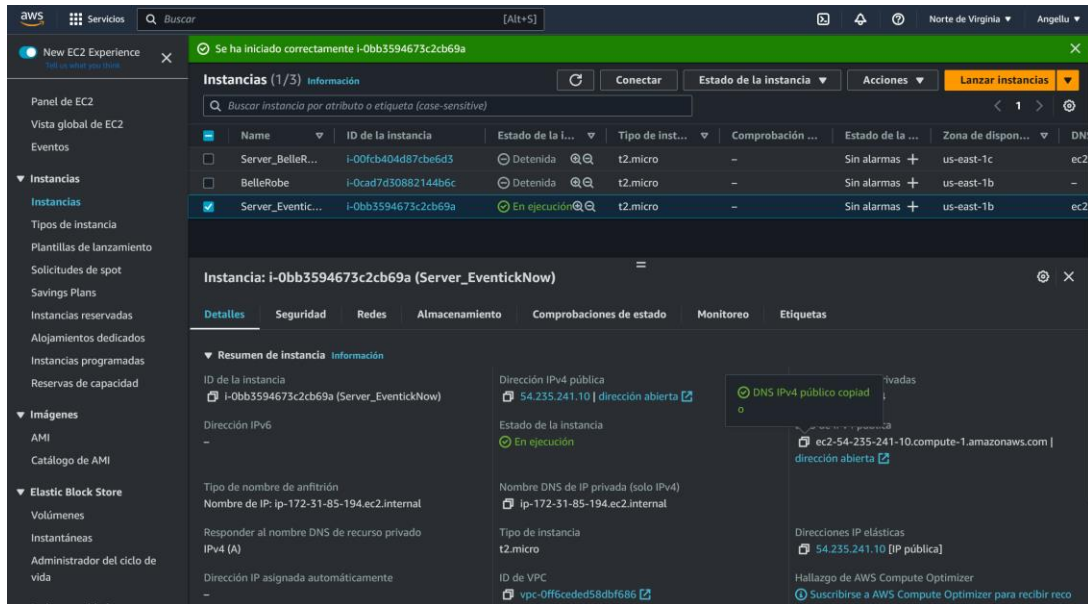


El presente trabajo ha sido elaborado por alumnos de la Ingeniería en Redes Inteligentes y Ciberseguridad de la Universidad Tecnológica del Norte de Guanajuato y se encuentra bajo la licencia de Atribución-NoComercial 4.0 Internacional de Creative Commons, por lo que está permitido compartir adaptaciones de la obra y comunicar públicamente esta obra respetando las siguientes condiciones:

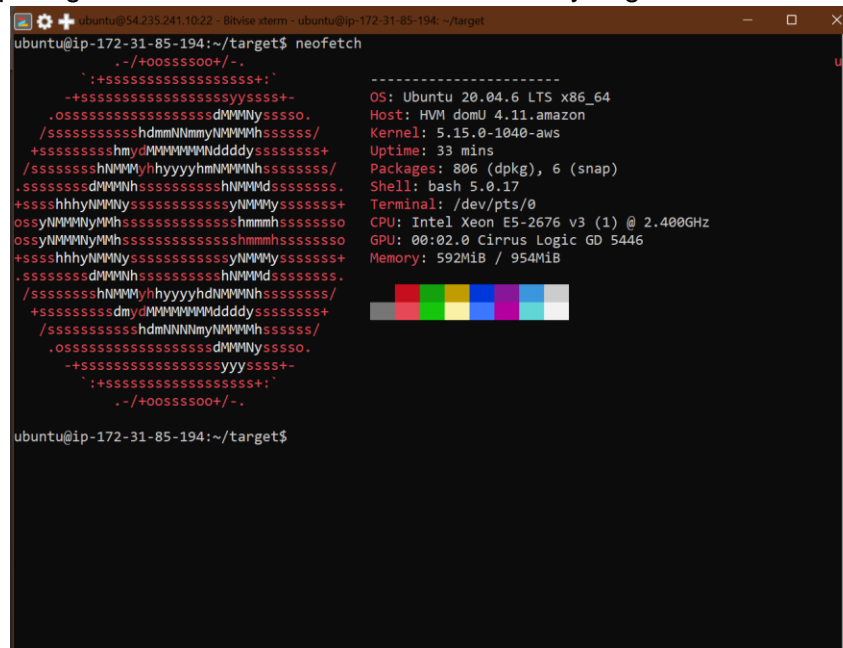
- El contenido de este informe puede ser reproducido de forma parcial o total por terceros, citando su procedencia y autor.
- El autor o autores de la obra no brindan apoyo al tercero, ni apoyan el uso que haga del material.
- Este trabajo y los trabajos derivados pueden ser distribuidos, copiados y exhibidos siempre y cuando su uso no tenga fines comerciales

Servidor de aplicaciones

Para el despliegue en la nube se utilizaron instancias de aws, la cual cuenta con una capa gratuita y fue perfecta para el despliegue de la aplicación.



La implementación de la aplicación web se realizó en el sistema operativo Ubuntu Server en su versión 20.04 es una LTS (Long Term Support), lo que significa que se proporcionará soporte y actualizaciones de seguridad durante cinco años, lo que es esencial en entornos de servidor para garantizar un funcionamiento continuo y seguro.



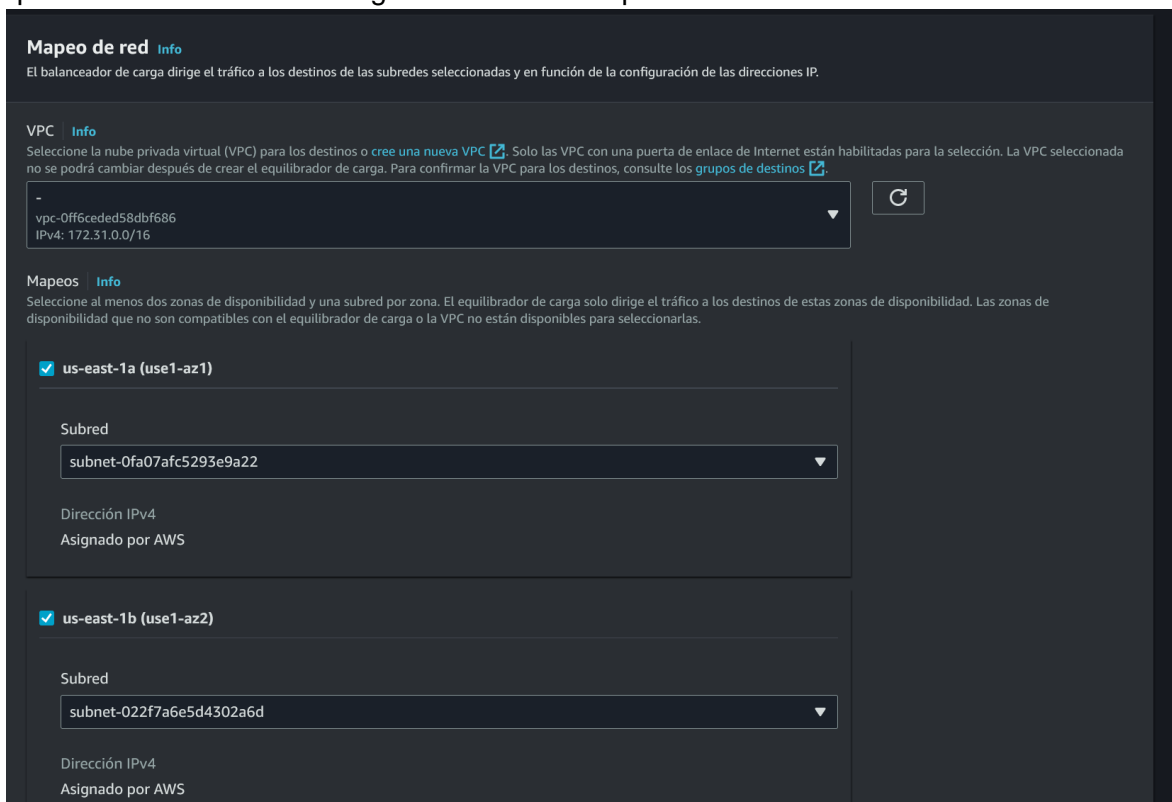
Servidor de Base de datos

Para el gestor de base de dato se decidió utilizar MySQL, el cual está diseñado para ser rápido y eficiente. Ha sido optimizado a lo largo de los años para manejar grandes cantidades de datos y transacciones de manera eficiente, lo que lo convierte en una opción sólida para aplicaciones que requieren un buen rendimiento de base de datos, además de la perfecta compatibilidad con la aplicación.

```
ubuntu@ip-172-31-85-194:~/target$ mysql --version
mysql Ver 8.0.33-0ubuntu0.20.04.4 for Linux on x86_64 ((Ubuntu))
ubuntu@ip-172-31-85-194:~/target$
```

Balanceador de Carga

Un balanceador de carga es un componente de red o software que distribuye el tráfico entrante entre múltiples servidores o recursos, con el objetivo de mejorar la eficiencia, la disponibilidad y el rendimiento de un sistema o aplicación. Su función principal es distribuir la carga de trabajo de manera equitativa entre los servidores en un grupo o clúster, evitando que un servidor se sobrecargue mientras otros permanecen subutilizados.



Mapa de red [Info](#)

El balanceador de carga dirige el tráfico a los destinos de las subredes seleccionadas y en función de la configuración de las direcciones IP.

VPC [Info](#)

Seleccione la nube privada virtual (VPC) para los destinos o [cree una nueva VPC](#). Solo las VPC con una puerta de enlace de Internet están habilitadas para la selección. La VPC seleccionada no se podrá cambiar después de crear el equilibrador de carga. Para confirmar la VPC para los destinos, consulte los [grupos de destinos](#).

vpc-0ff6ceded58dbf686
IPv4: 172.31.0.0/16

Mapeos [Info](#)

Seleccione al menos dos zonas de disponibilidad y una subred por zona. El equilibrador de carga solo dirige el tráfico a los destinos de estas zonas de disponibilidad. Las zonas de disponibilidad que no son compatibles con el equilibrador de carga o la VPC no están disponibles para seleccionárselas.

☒ **us-east-1a (use1-az1)**

Subred
subnet-0fa07afc5293e9a22

Dirección IPv4
Asignado por AWS

☒ **us-east-1b (use1-az2)**

Subred
subnet-022f7a6e5d4302a6d

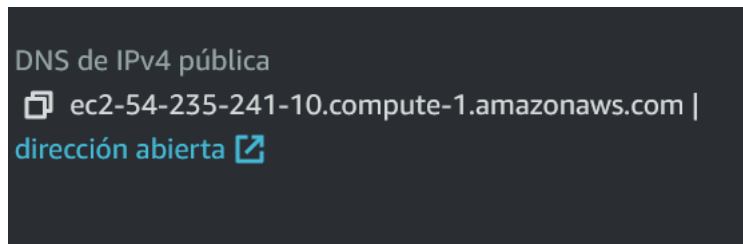
Dirección IPv4
Asignado por AWS

En la imagen anterior se identifica las 2 subredes configuradas para el balanceo de carga correspondiente para las instancias

Dominio

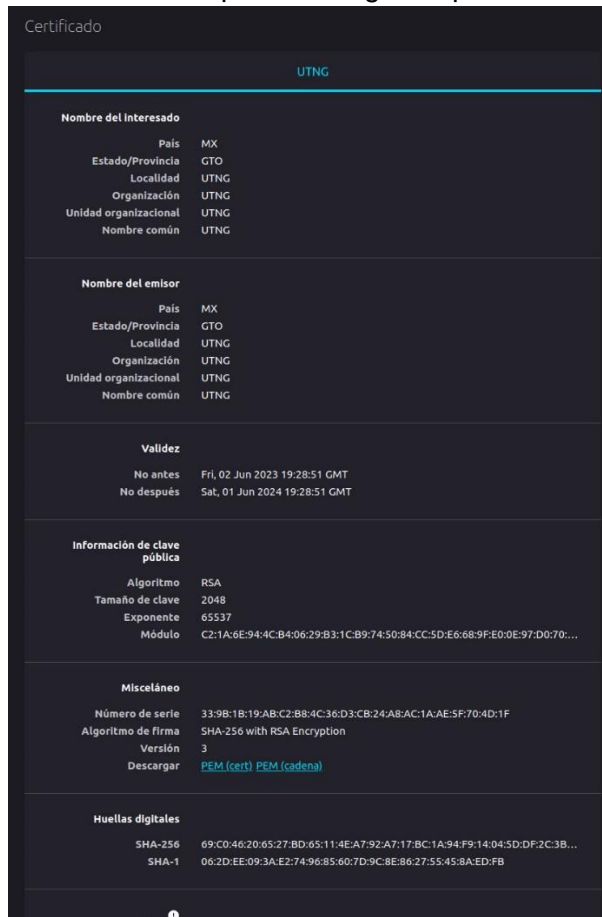
Para el servidor DNS venia implementado en la capa gratuita solamente se configuro en la instancia para redes.

Un servidor DNS (Sistema de Nombres de Dominio, por sus siglas en inglés) es un componente esencial de la infraestructura de Internet que traduce los nombres de dominio legibles por humanos en direcciones IP numéricas que las computadoras utilizan para identificar y acceder a recursos en la red. En otras palabras, actúa como una especie de "libro de direcciones" que permite que las personas utilicen nombres de dominio como "www.ejemplo.com" en lugar de tener que recordar las direcciones IP numéricas asociadas, como "192.168.1.1".



Seguridad

Certificado SSL para Redirigir del puerto 80 al 443 (https)



Denegación de tráfico ICMP

Se deniega todo el tráfico de ICMP para evitar ataques de denegación de servicio a la aplicación WEB

```

C:\Users\salva>ping ec2-54-235-241-10.compute-1.amazonaws.com

Haciendo ping a ec2-54-235-241-10.compute-1.amazonaws.com [54.235.241.10] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 54.235.241.10:
    Paquetes: enviados = 3, recibidos = 0, perdidos = 3
    (100% perdidos),
Control-C
^C
C:\Users\salva>
  
```

Como se logra ver en la imagen anterior el ping se deniega de forma exitosa.

Filtrado de puertos

Se dejan solamente abiertos los puertos que se necesitan para el funcionamiento de la aplicación web

Nombre	ID de la regla del grupo d...	Intervalo de pu...	Protocolo	Origen	Grupos de se
-	sgr-0a2392513547964c9	443	TCP	0.0.0.0/0	launch-wizar
-	sgr-01633b85f8fa83055	80	TCP	0.0.0.0/0	launch-wizar
-	sgr-0611e3056e18d5634	22	TCP	0.0.0.0/0	launch-wizar
-	sgr-0c6ab6cb6db1fea25	9090	TCP	0.0.0.0/0	launch-wizar
-	sgr-0ad6243798cb75093	19999	TCP	0.0.0.0/0	launch-wizar
-	sgr-0f233a05054d71933	8080	TCP	0.0.0.0/0	launch-wizar

Key SSH

Se deniega el acceso de SSH por contraseña, por lo que solamente las personas que tenga la llave podrán ingresar al servidor.

```

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAgmvmch5GTxGz1jTWYf6ni1G4dygRts+mjj7gv3cHfuB1Eijh
fQypB65wA5/noBbz1T7vP8bD2BGPzMDJoC3yV5wSYLA8V0sDkcumJivwJJLnfn8
XFuPWiqFuNrot8kE194S6QVapjD2RkwmU4MPg9PTtrcmaLaS5udR35546748EQvd
bPFm60GISHqnF2st1HrKnnxSjDbn1ZEIRiTFGPKhiOLQtCNXOSxKM8t6gPiRi+et
Gqanzj4k6TtT4KFQh3NpaAIS4UAPHXKHI8jrJW8bWkSd5sVST3qxXhJMcFU3Wpg
dpXN/4EpWVs7zJpufgtUiJWzyQYiPvKYJjwQIDAQABoIBAHOc9ajnN8F6/zIz
ZihxM078GcWnv8K1ysyieGHGukVxOTTO9/yj3nIoN/S8INY9AsoJwYt5qPg3nb7g
0P/AXEqoBwm2FgsffcxioKtD1J8kjMfo2jeRFLawwViJppnhPiHRiQFkl+SIQ62E
NVFFeDtm7XCvMqiFXRkVaRv5xohLqOn9+/k3f61w+hN8Vx4c8MXK+6RI8oeHeD4
Wbagg4m5B2MeUfNUVHPMDxXng4ne6t45L3G1lyuKBaRY8ppiNuQqnMqJPp8NY/NG
kpoNYkzDUNcAVNmTJJ20yPJ7AubeD+cJtaumZWESjGVASbjOGEvD4fNv/v3ROKe
Sz3MjJ0CgYEA3YPFKy6EvZHKQ1fAifRzF7GRDscpQqk9AhS52jUp2hYfmdG6yi
Rv4EWHcsx9u5DnSOFsnLARMsTPLd79Wtkgv0XgqideZ814jn4vIpc3aajETcHsGX
Z6Gpp9Me94yubIJ8BrzP4kBsCDR8iWgw1Cdw6Du77HrC7c2WGPnxvcCgYEA1rm1
FiY79M7JjIvzTpC3vq59hYXIMwQfjjeM5eafCSnNOXWFWXqdXGmwcHnQPHGF3CJ
eX+bit4WmDB+ISB5koQ1weKFAfpVW1OT9zP5R5TRp4o4Dz3uba8PJOUa04+RwQwY
qd5CZQUZxld60sx5JKAaGTyie1x/7Y7nL7Ct5QcGyEAu6oBBn5YksngmeSLUyYt
BX1dezyHemQqfXLRoM3u712DhMiSipZ1VAVS+NbbRrXUEXXGqD5oD6DKCX/7
1nluQ6w60Su9bhvcafZEa7+VwzSTT7Mu8+rv8nBYEd0rgF5jeMnJTKLLY4A3x21
SYN1k1bY9JVKicizHIkNS0CgYAWF6ZJvTvw7rBwXT7QcAe5MzrqRy6wm5wcdAO
c9w88gxoHoAgps2U5VGx+LwxwW7NpLshyeh81EzvhbwXbmfdAaMRH6irP4wFVMLN
axrQuS15yzKoWUWHYi9wEvyyjWknc5+79ShL1R7gdcFkEIVBoY+cvZ8nQ8Zn2sgmE
3fq/JQK8gApMZ+A7ydr24mRmFxc16XIutV1Bxb1LQojceqq2cA1QQU7dWufZQkPO
1trht0sYamEGh1fOGEP0K81UoS03ZNpHeU82dGSjWckg/++SVXICJK/gb0YGP7m
eL2YmL5p3n6sNklipBdbuggwE+83ToulPZH+wIpcw75WSyGACxeA
-----END RSA PRIVATE KEY-----
  
```

Programa de respaldo con encriptación

Se realiza un programa de respaldo para la aplicación web y la base de datos el cual está encriptado con el protocolo aes-256-cbc, con el fin de evitar que la información sensible de los usuarios caiga en malas manos.

```

GNU nano 4.8                                program_resp.sh
#!/bin/sh

cd /home/ubuntu/app/DesarrolloWebIntegral-Proyecto/FrontendEventickNow
mysqldump -u eventick -peventick Eventick > resp_$(date +%d%k%y_%H%M).sql
tar -zcf /home/ubuntu/resp/respaldo_$(date +%d%k%y_%H%M).tar.gz --exclude="node_modules" *
rm resp_*
cd /home/ubuntu/resp
openssl aes-256-cbc -a -salt -in respaldo_$(date +%d%k%y_%H%M).tar.gz -out resp_$(date +%d%k%y_%H%M).tar.gz.enc -k V$!D2K
rm respaldo_$(date +%d%k%y_%H%M).tar.gz
  
```

El programa se agrega al crontab para que el respaldo se realice de forma automática a las 22:00 hrs

```

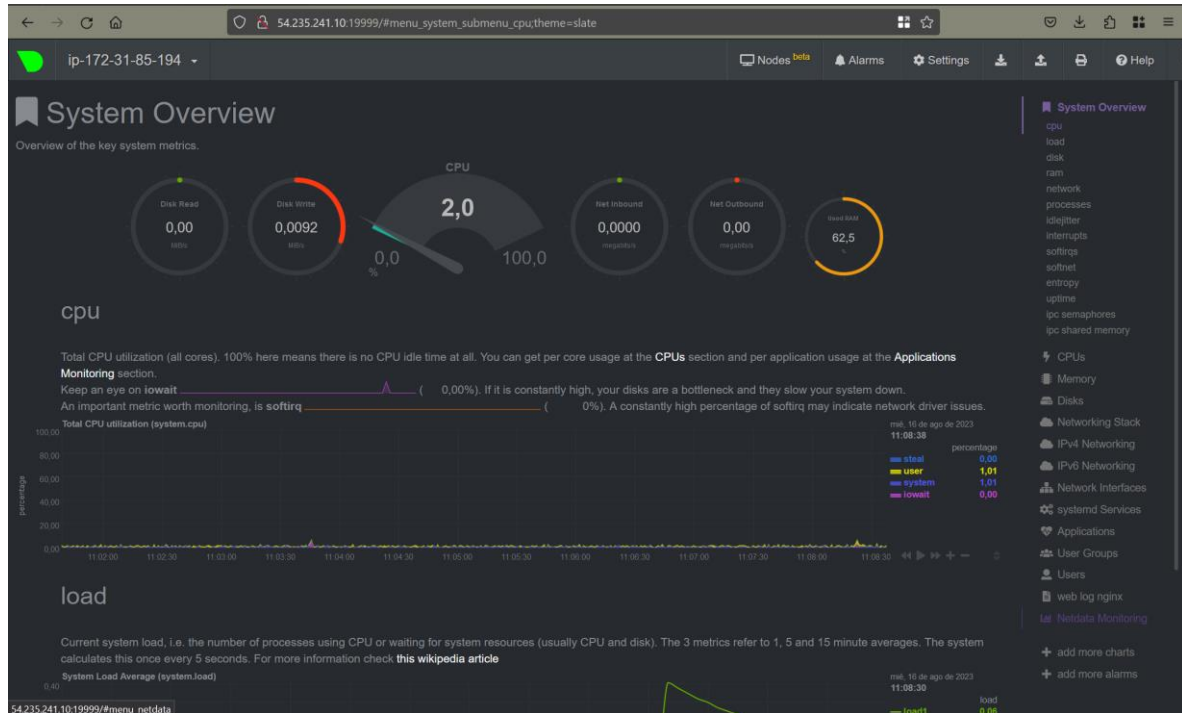
GNU nano 4.8                                /etc/crontab
/etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file,
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
00 22 * * * root /home/ubuntu/resp/program_resp.sh
  
```

Monitoreo de servidores

Se realiza la instalación de software de monitoreo para servidores el cual permite al administrador darse cuenta de ataques DDOS, DOS, fuerza bruta, etc.

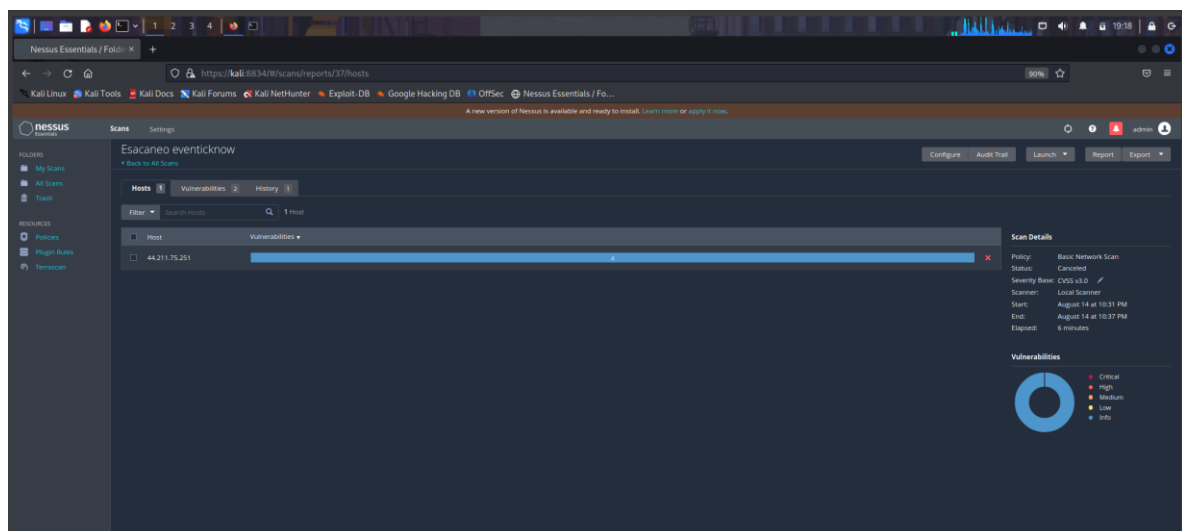


Análisis de Vulnerabilidades

¡¡¡IMPORTANTE!!!

El análisis realizado a continuación fue hecho siguiendo las normas del Hacking Ético y en un entorno controlado y con autorización del dueño del servidor (Equipo de Redes), cualquier análisis o ataque no autorizado puede ser penalizado legalmente.

Se realizó una prueba de vulnerabilidades la cual fue exitosa y no se encontró ninguna vulnerabilidad en el servidor solamente información.



Enlace de despliegue de la aplicación

DNS: ec2-54-235-241-10.compute-1.amazonaws.com