



INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Seguridad en Servicios

Practica 2

ALUMNO:

Rogelio Cristian Punzo Castro **21120245**

PROFESOR:

Ruben Lara Barcenas

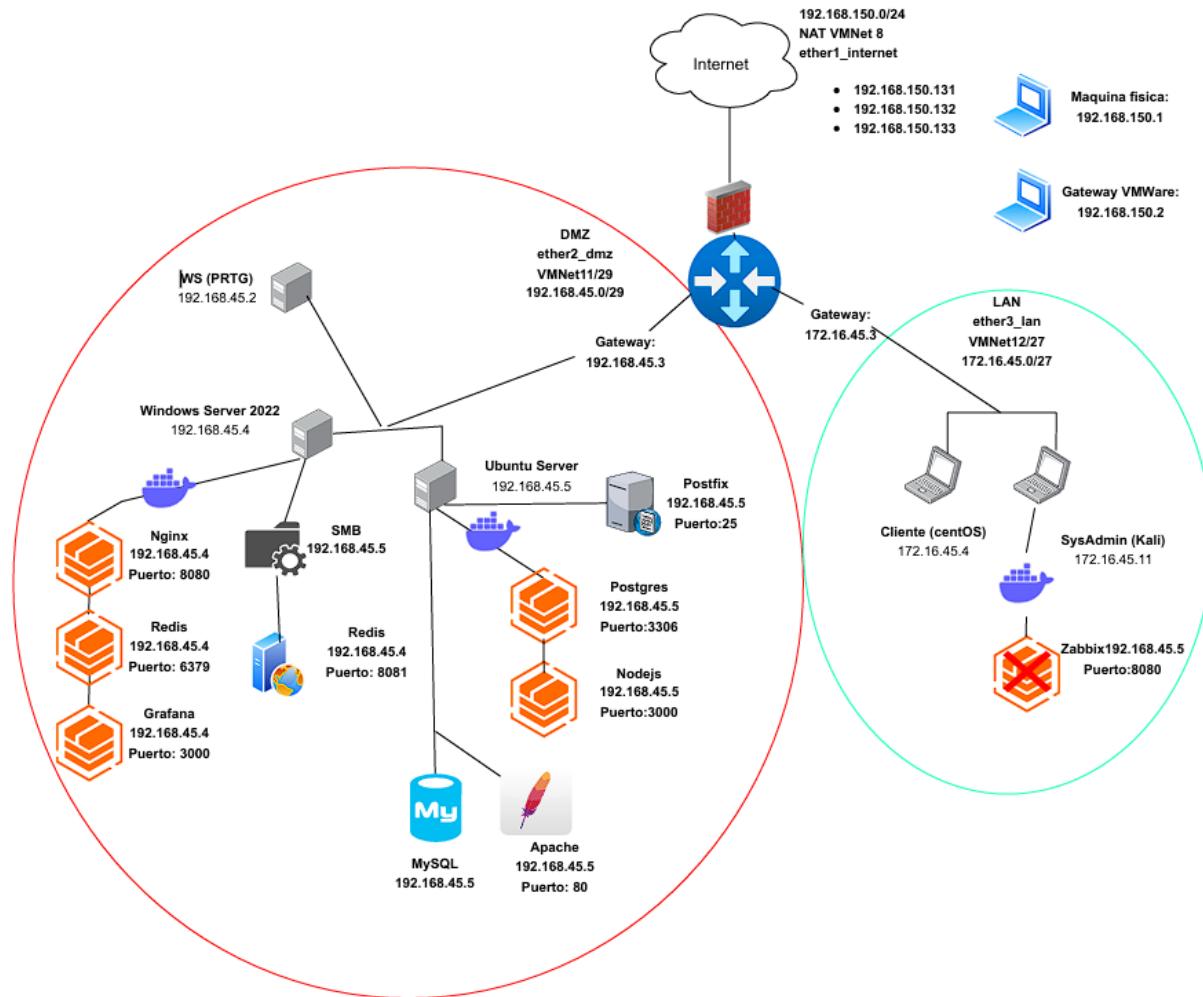
MORELIA, MICHOACÁN

(Marzo 2025)

Contenido

Diseño de red	2
Usuarios y contraseñas	2
Escaneos NMAP	3
Servicios y microservicios	6
Matriz de Riesgos	7
Herramientas de monitoreo	9
Conclusiones:	13

Diseño de red



Usuarios y contraseñas

Maquina Windows Server 2022:

- Usuario: Administrador
- Contraseña: Admin123*

Maquina Ubuntu

- Usuario: ubuntu
- Contraseña: Urano123*

Maquina Kali Linux

- Usuario: kali00
- Contraseña: kali00

Maquina Cliente (CentOS)

- Usuario: cent00s
 - Contraseña: Cent00s55

Servidor PRTG:

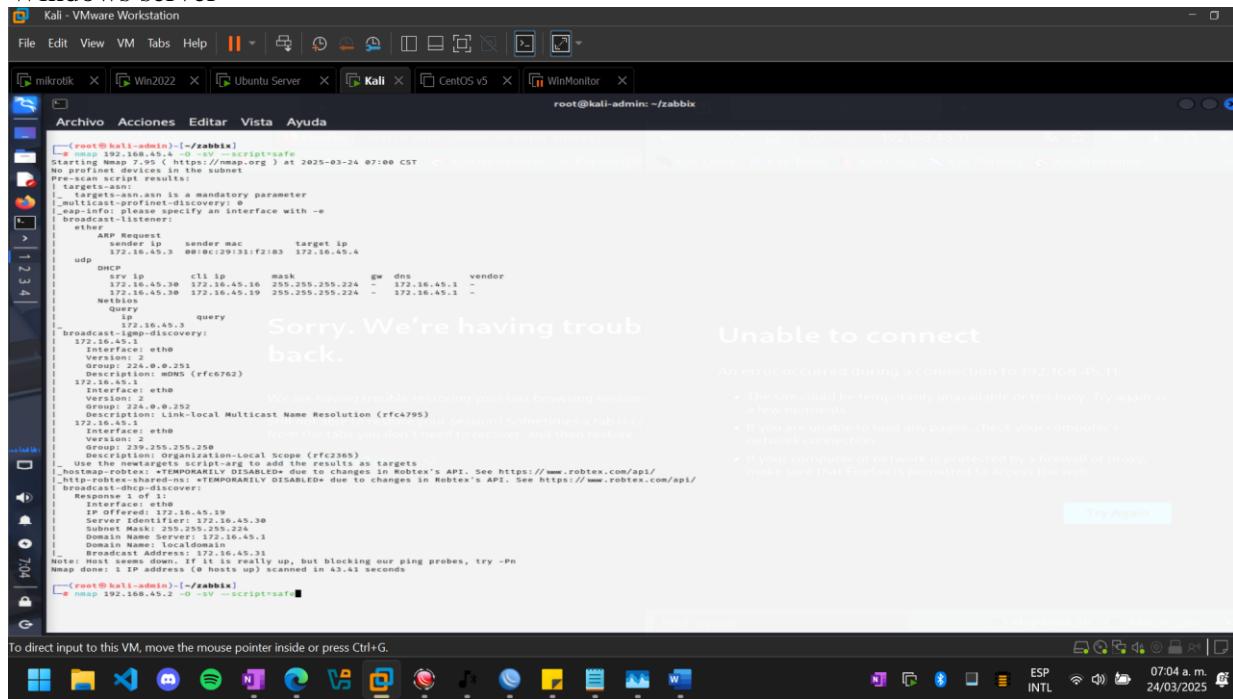
- **Usuario:** prtadmin
 - **Contraseña:** PEPIT00*

Certificado HTTPS WS:

- **winiis123***

Escaneos NMAP

Windows server



Ubuntu server:

The screenshot shows a Kali Linux desktop environment with several windows open. The terminal window at the bottom has the following content:

```
[root@kali-admin: ~]# zabbix
[+] nmap -v 192.168.45.5 -o >script-safe
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-24 06:43 CST
Nmap scan type: script
Pre-scan script results are temporarily DISABLED due to changes in Nmap's API. S
ee https://www.robtex.com/api/ for more information.
Script results are temporarily DISABLED due to changes in Nmap's API. S
ee https://www.robtex.com/api/ for more information.
API See https://www.robtex.com/api/
[broadcast-icmp-discovery:
Interface: eth0
Version: 4.0.0
Group: 224.0.0.251
Description: MONG (rfc6762)
172.16.45.1
Interface: eth0
Version: 4.0.0
Group: 224.0.0.252
Description: Link-local Multicast Name Resolution (rfc4795)
172.16.45.1
Interface: eth0
Version: 4.0.0
Group: 239.255.255.250
Description: Multicast Listener Discovery (rfc3463)
Use the newtargets script arg to add the results as targets
[-]Warning: You must specify an interface with -e!
[broadcast-listener:
eth0
      EIGRP Request
      ARP Request
      sender mac          target ip
      172.16.45.3 00:0c:29:51:ff:ec  172.16.45.4
      172.16.45.1 00:0c:99:9b:c0:ec  172.16.45.3
      udp
      DHCP
      SRV ip       clt ip        mask      gw      dns      ve
      172.16.45.30 172.16.45.19  255.255.255.224  -  172.16.45.1  -
      172.16.45.30 172.16.45.20  255.255.255.224  -  172.16.45.1  -
      netbios
      CNAME
      ip           query
      targets-asn
      -target-asn-param is a mandatory parameter
      broadcast-icmp-discover:
      Response 1 of 1:
      IP Offered: 172.16.45.19
      Interface: eth0
      Subnet Mask: 255.255.255.252
      Domain Name Server: 172.16.45.1
      Default Gateway: 172.16.45.1
      Broadcast Address: 172.16.45.31
      Multi-Homed Preferred: 172.16.45.1
      Nmap scan Report for 192.168.45.5
```

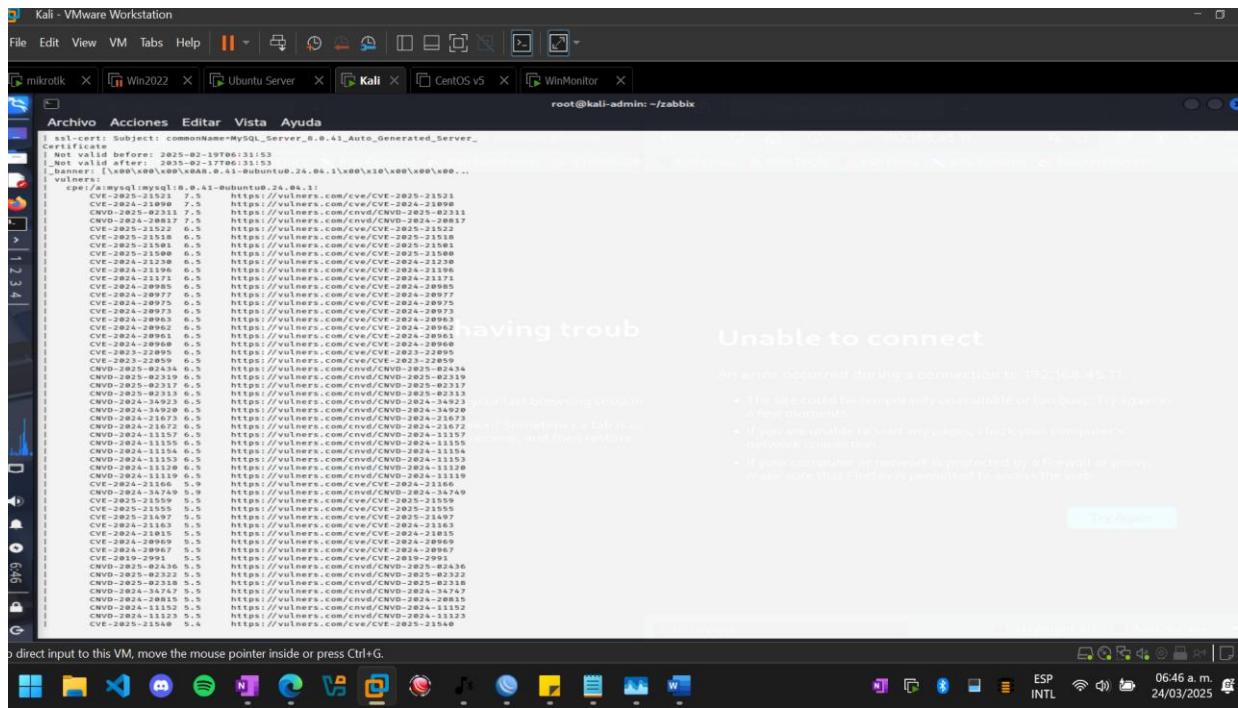
In the center of the screen, there is a large watermark-like message: "Sorry, We're having trouble connecting to your network". To the right of this message, another message reads: "Unable to connect. An error occurred during a connection to 192.168.45.5". Below these messages, there are several bullet points with explanatory text.

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

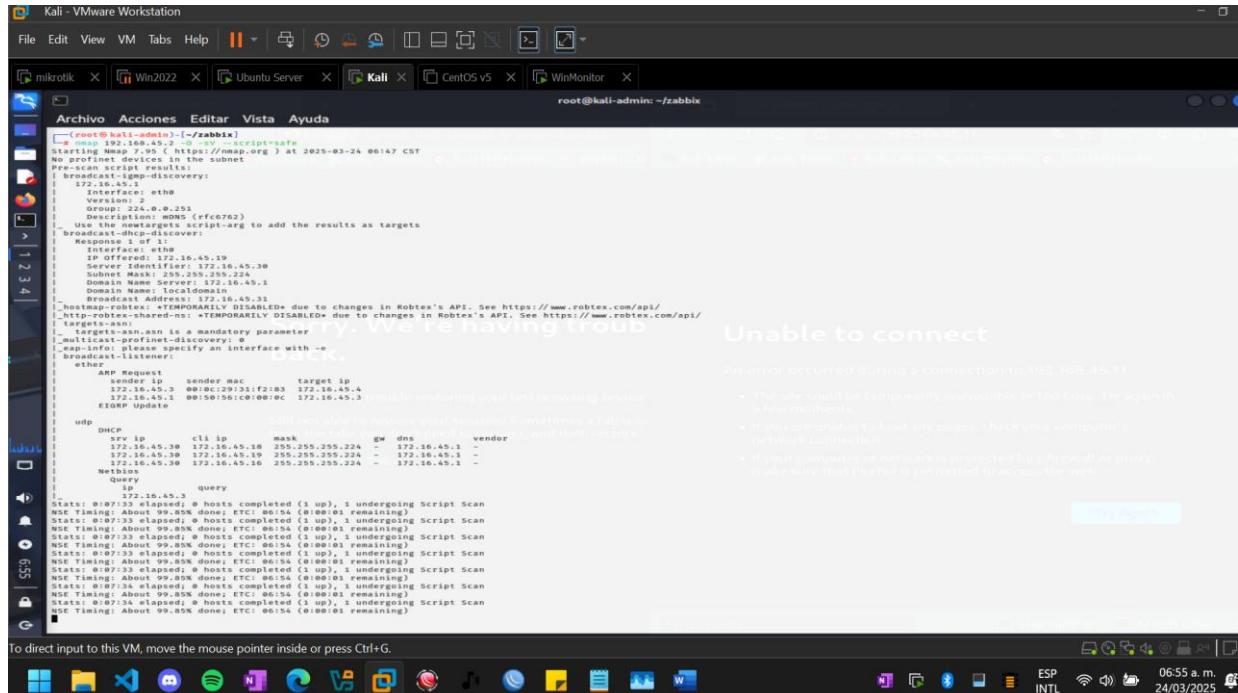


To return to your computer, move the mouse pointer outside or press Ctrl+Alt.





PRTG server:



Servicios y microservicios

La empresa cuenta con una infraestructura compuesta por diversos servicios críticos y microservicios distribuidos entre máquinas físicas y contenedores Docker, sobre sistemas operativos Windows Server y Ubuntu Server.

SNMP: Es el protocolo que nos va a permitir recolectar datos de dispositivos de red (servidores, routers, switches) en tiempo real, facilitando la supervisión unificada.

- ◆ Detección Rápida de Fallos: Alertas automáticas (traps SNMP) ante problemas como:

- Alta CPU/memoria.
 - Caída de enlaces.
 - Errores en interfaces.

Servicios:

Servicio	Puerto	Instalación	Descripción
IIS (Web Windows Server)	8081	Windows Server	Servicio web principal
SMB (Compartida)	445, 137-139	Windows Server	Compartición de archivos
Apache	80	Ubuntu Server	Servidor web adicional

<i>MySQL</i>	3306	Ubuntu Server	Base de datos relacional
<i>Postfix</i>	25	Ubuntu Server	Servidor de correo

Microservicios:

Microservicio	Puerto	Instalación	Descripción
<i>Redis</i>	6379	Docker (Windows Server)	Base de datos no relacional
	3000	Docker (Windows Server)	Monitorización y visualización
<i>Grafana</i>	8080	Docker (Windows Server)	Servidor proxy inverso
	Default (5432)	Docker (Ubuntu Server)	Base de datos relacional
<i>PostgreSQL</i>	3000	Docker (Ubuntu Server)	Backend API

Archivos Log e Informes

Para cada servicio y microservicio, se capturaron logs relevantes y reportes de estado:

Servicio/Microservicio	Logs Generados	Herramienta usada
<i>IIS</i>	C:\inetpub\logs\LogFiles	IIS Logs
	Eventos en Visor de Eventos (Windows Logs -> Security/Sharing)	Visor de eventos
	/var/log/apache2/access.log y /var/log/apache2/error.log	Apache Logs
	/var/log/mysql/error.log	MySQL Logs
	/var/log/mail.log	Mail Logs
	Docker logs + /data/redis/redis.log	Docker, Redis log config
	Docker logs /var/lib/grafana/log	Docker logs
	Docker logs /var/log/nginx/access.log y error.log	Docker, Nginx logs
	Docker logs /var/lib/postgresql/data/pg_log	PostgreSQL logs
	Docker logs con salida estándar + archivos /app/logs	Docker logs, winston/logger en app

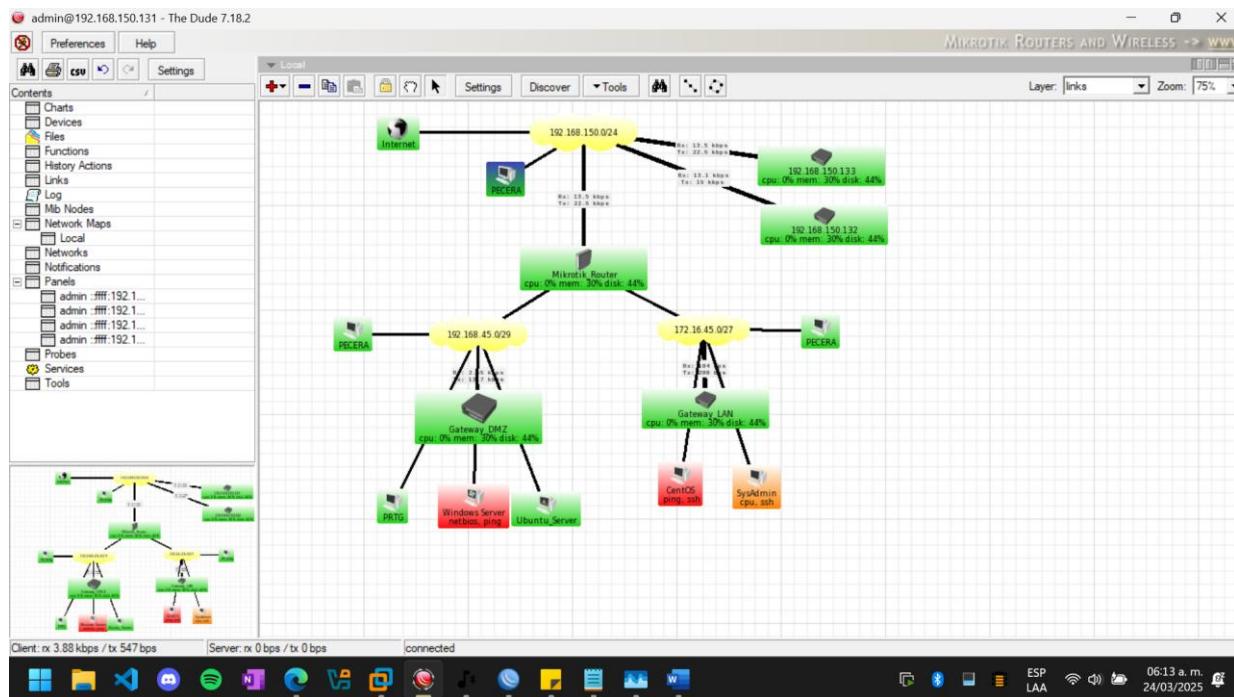
Matriz de Riesgos

Riesgo Identificado	Servicio/Microservicio Afectado	Impacto	Probabilidad	Mitigación
----------------------------	----------------------------------------	----------------	---------------------	-------------------

<i>Acceso no autorizado (SMB)</i>	SMB	Alto	Medio	Restricción IP, autenticación
<i>Inyección SQL</i>	MySQL, PostgreSQL, Node.js	Alto	Medio	Validación entrada, firewall, roles limitados
<i>Denegación de servicio</i>	Todos	Alto	Alto	Limitar conexiones, balanceo, monitoreo
<i>Vulnerabilidad en contenedores</i>	Docker-based services	Medio	Alto	Actualización periódica, imágenes oficiales
<i>Certificados autofirmados</i>	IIS, Nginx	Bajo	Alto	Uso de certificados válidos
<i>Fallo en SMTP (Postfix)</i>	Postfix	Medio	Bajo	Backup, failover
<i>Saturación de recursos</i>	Redis, MySQL, Apache	Alto	Medio	Monitorización activa (Grafana)
<i>Configuración errónea</i>	Todos	Medio	Medio	Revisión y automatización de despliegue

Herramientas de monitoreo

The Dude



Envio de mensaje telegram:

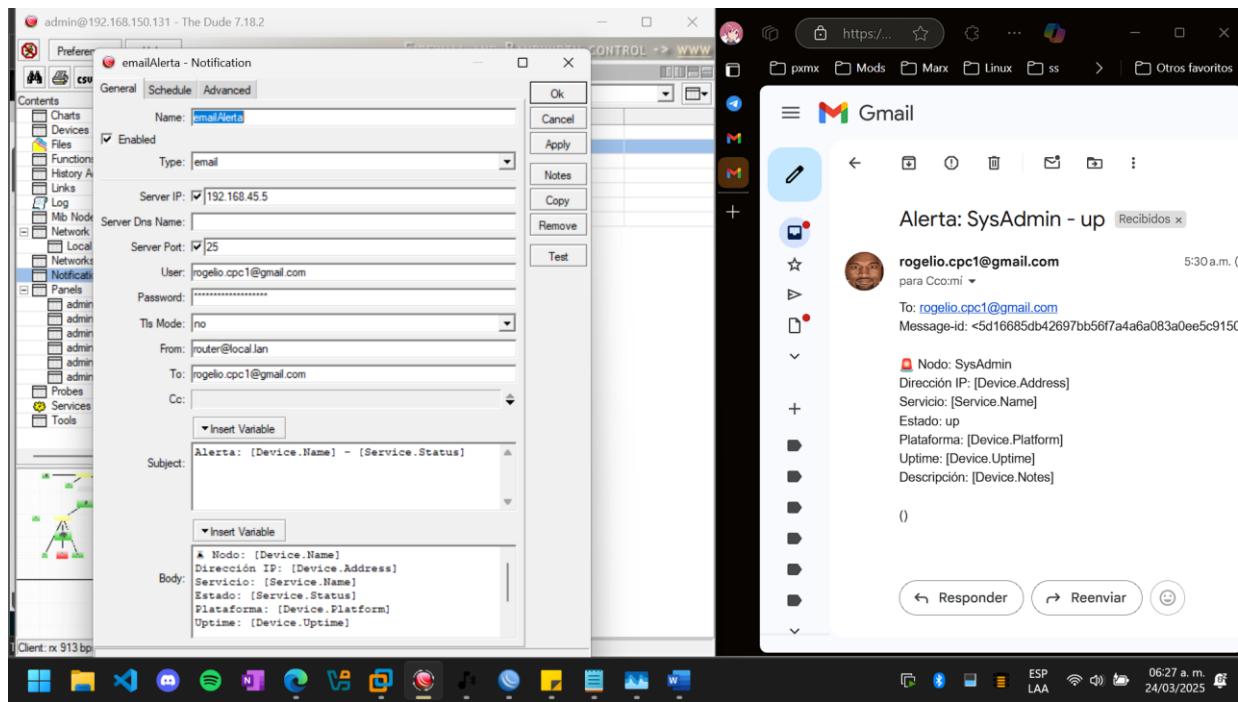
The left pane shows the configuration of a **Telegram.Notification_BOT** object in WinMonitor. The configuration includes:

- Nombre de plantilla:** Telegram.Notification_BOT
- Estado del monitoreo:** Iniciado (predeterminado)
- Horario:** Ninguno
- Gestión de notificaciones durante una pausa programada:**
 - Recopilar notificaciones y enviarlas cuando se vuelve a activar (predeterminado)
 - Descartar notificaciones durante el estado Pausado

The right pane shows a Telegram message window with three notifications from a bot named "Red mkt". The notifications are:

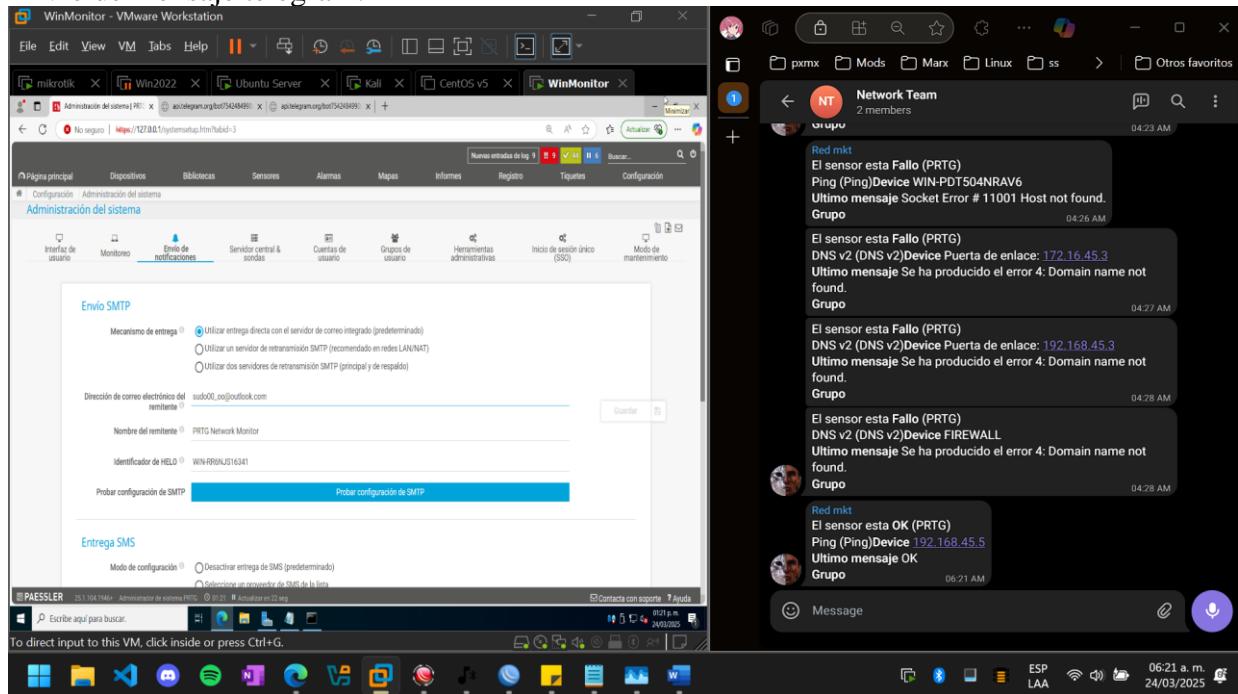
- Este es un mensaje SMS de prueba procedente de PRTG 03:38 AM
- Mar/24/2025 10:41:33
Nodo: SysAdmin
IP: [Device Address]
Servicio: [Service Name]
Estado: up
Plataforma: [Device Platform]
Uptime: [Device Uptime]
Descripción: 04:41 AM
- Mar/24/2025 10:51:06
Nodo: SysAdmin
IP: [Device Address]
Servicio: [Service Name]
Estado: down
Plataforma: [Device Platform]
Uptime: [Device Uptime]
Descripción: ICMP error received (6)host unreachable 04:51 AM
- Mar/24/2025 11:30:03
Nodo: SysAdmin
IP: [Device Address]
Servicio: [Service Name]
Estado: up
Plataforma: [Device Platform]
Uptime: [Device Uptime]
Descripción: 05:30 AM

Envio de correo:

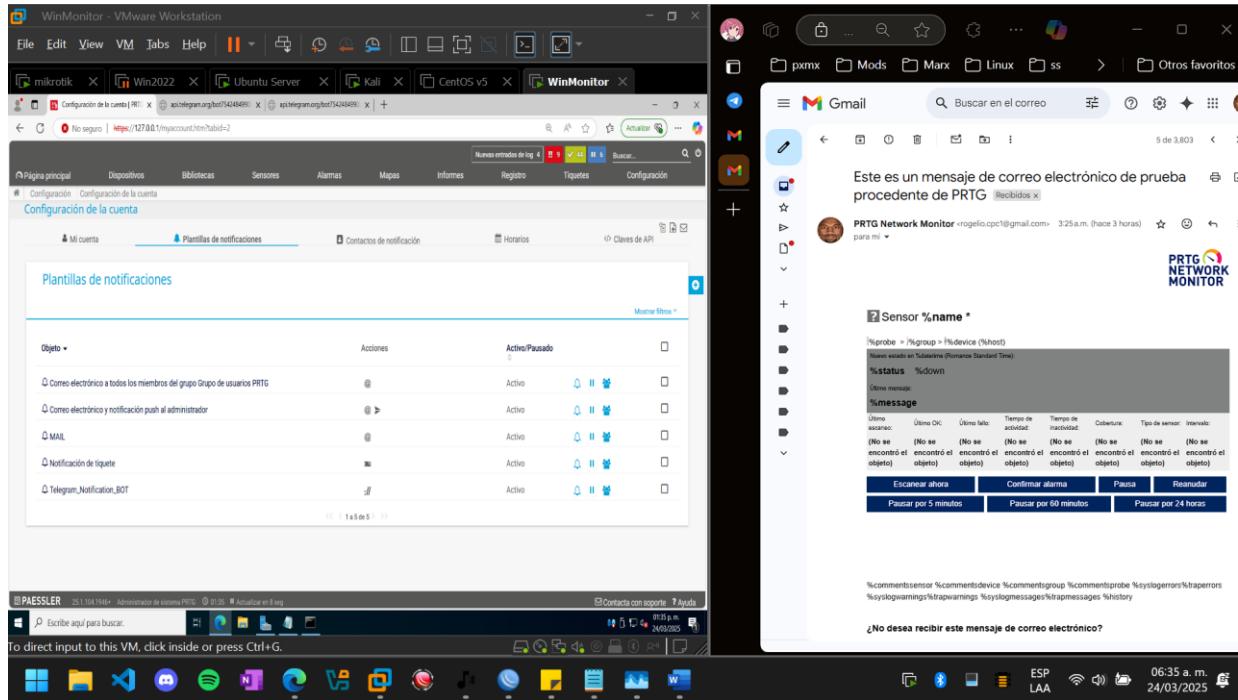


PRTG

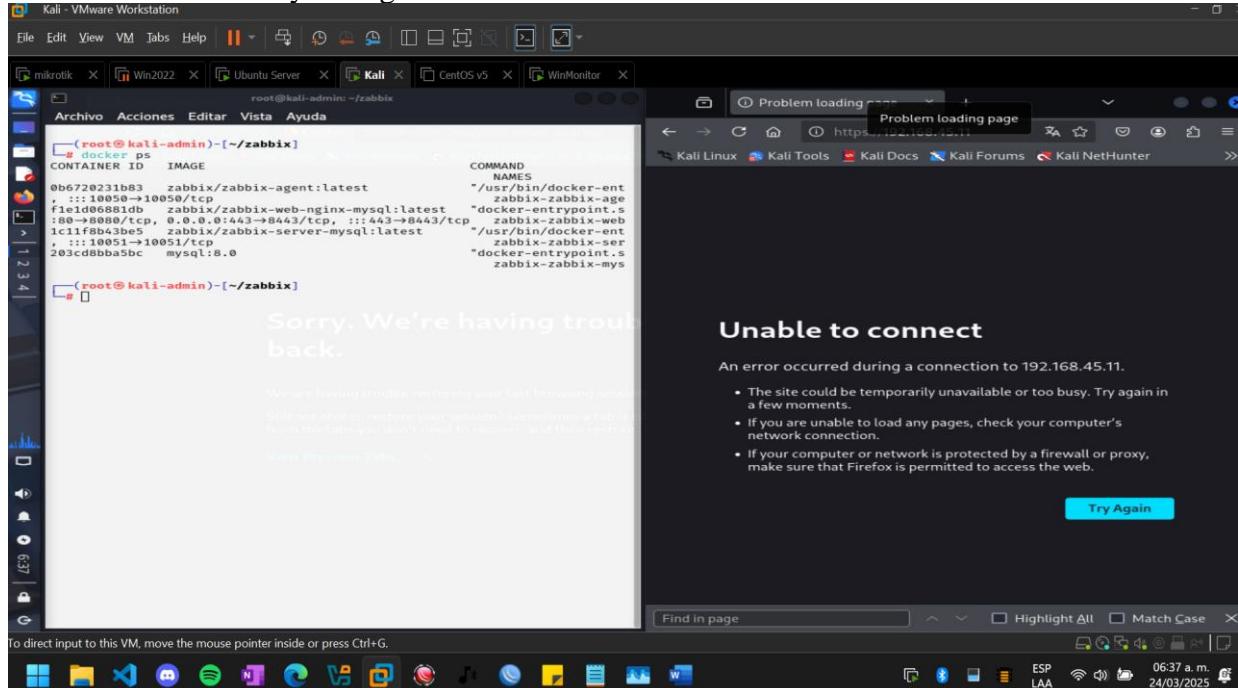
Envio de mensaje telegram:



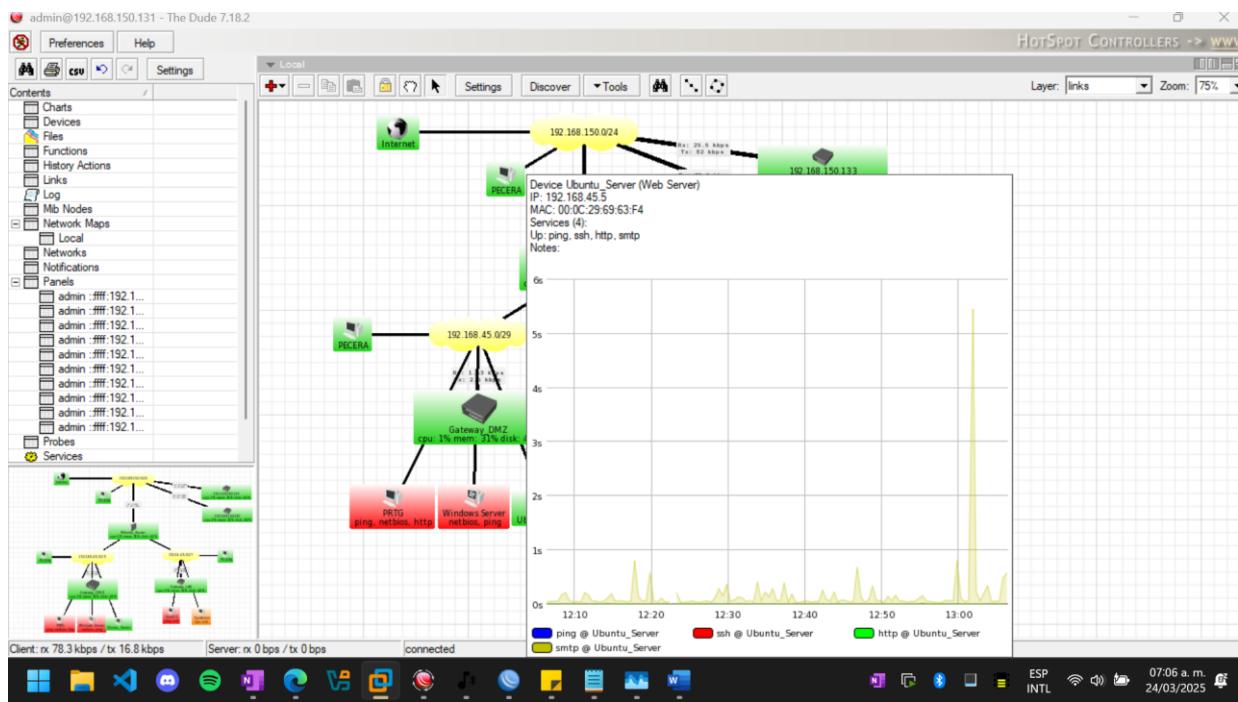
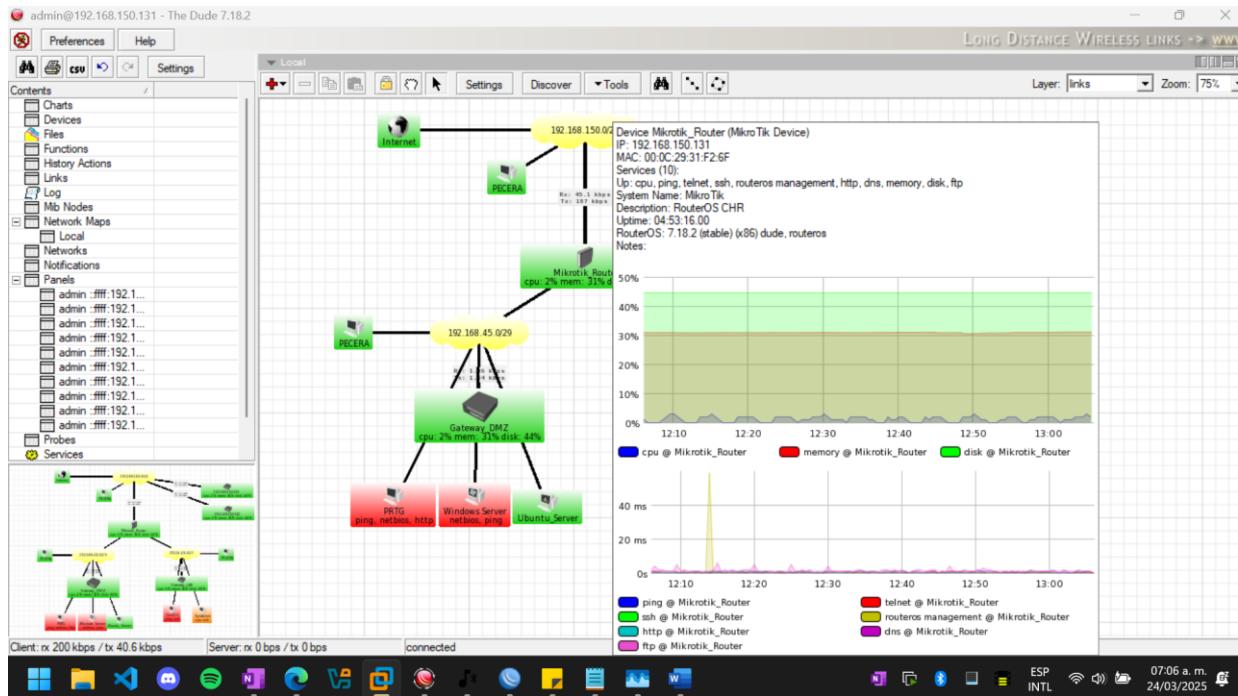
Envio de correo:



Zabbix
Se hizo la instalación y configuración.



Pero no se logró conectar.



La resiliencia de los servicios y microservicios fue evaluada con base en su capacidad para soportar fallos, responder ante picos de carga y mantener la continuidad operativa frente a eventos adversos.

Capacidad de recuperación:

- Los servicios implementados en contenedores Docker demostraron gran flexibilidad para ser reiniciados rápidamente ante cualquier falla, lo que facilita su disponibilidad continua.
- Servicios críticos como **IIS, Apache y Postfix** respondieron adecuadamente después de pruebas de desconexión y reinicio, retomando su operación sin pérdida de datos, aunque por ejemplo postfix puede tardar un poco mas en iniciar.

Rendimiento sostenido:

- Microservicios como **Redis y Node.js** conservaron baja latencia incluso bajo simulación de múltiples solicitudes simultáneas.

Puntos de mejora:

- Se detectaron riesgos relacionados con el uso de certificados autofirmados, lo que podría comprometer la percepción de seguridad para los usuarios finales.
- El servicio SMB podría beneficiarse de políticas de acceso más estrictas y segmentación para evitar accesos no autorizados.

Conclusiones:

Implementar un sistema de monitoreo continuo, junto con la evaluación del rendimiento de los servicios y microservicios, ha demostrado ser un factor crítico para garantizar la alta disponibilidad, estabilidad y resiliencia de la infraestructura tecnológica de la empresa. Mediante herramientas como Grafana, Prometheus, logs estructurados y pruebas de estrés, se pueden obtener métricas precisas sobre tiempos de respuesta, consumo de recursos y capacidad de recuperación ante fallos, lo que permitió identificar tanto fortalezas como áreas de mejora. Algunos de los puntos mas importantes fueron que la mayoría de los servicios (Apache, SMB, Redis, Nginx) mostraron un comportamiento robusto incluso bajo cargas elevadas y escenarios de fallo simulado. También en que los contenedores gestionados con políticas de reinicio automático (`--restart unless-stopped`) demostraron una recuperación eficiente, minimizando la intervención manual. La supervisión en tiempo real permitió detectar anomalías (ej: picos de CPU en MySQL o lentitud en Postfix) antes de que escalaran a fallos críticos, reduciendo así el tiempo de inactividad no planificado. En si se puede

decir que el monitoreo continuo no solo mejora la operatividad, sino que también refuerza la seguridad, al detectar accesos no autorizados (ej: intentos de fuerza bruta en Apache) o configuraciones vulnerables (ej: Redis sin autenticación).