Propuesta y análisis de ciberseguridad

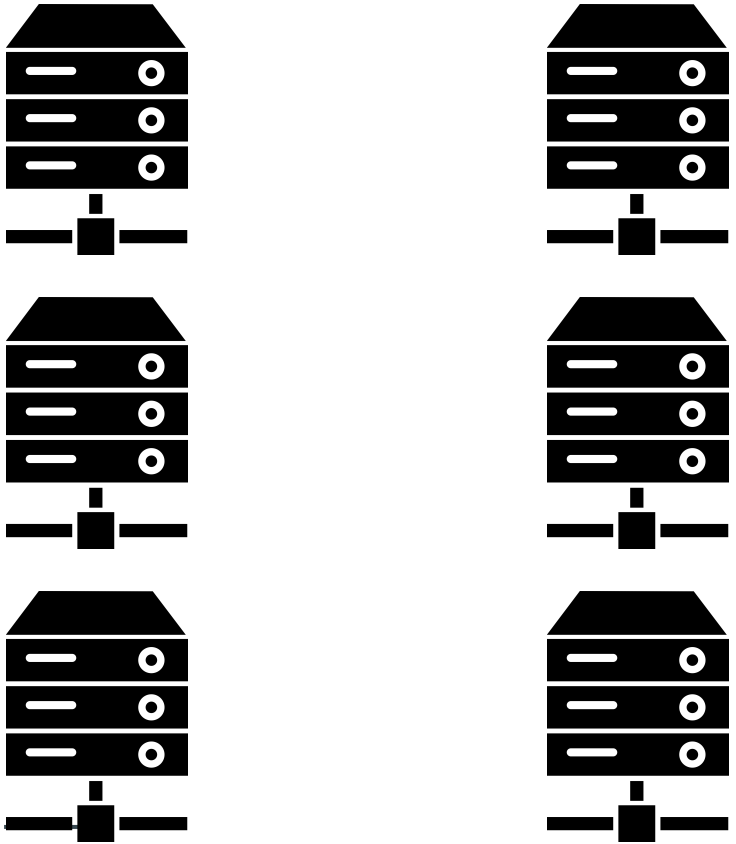
20 de marzo de 2024

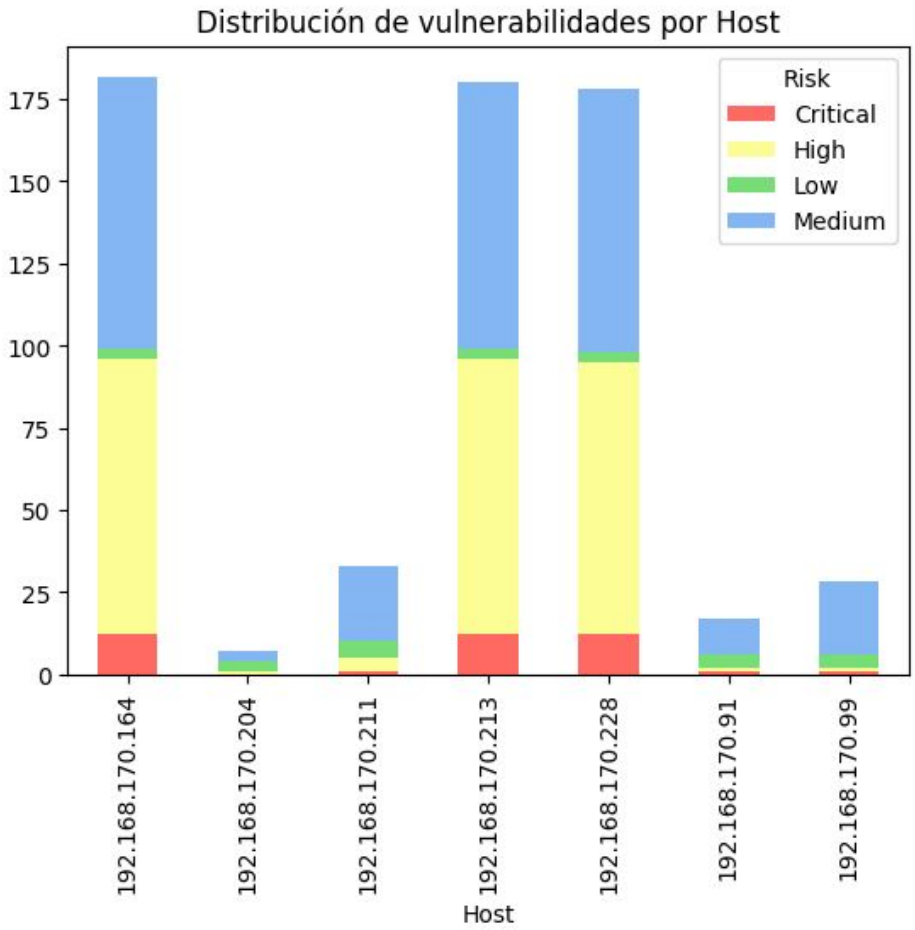
Objetivo del proyecto:

1. Identificar el problema de raíz y trabajar para eliminarlo.
2. Intentar solucionar la mayor cantidades de vulnerabilidades en el menos tiempo posible para no caer en un ataque cibernético.

Comprensión del estado actual

Equipos y sus vulnerabilidades



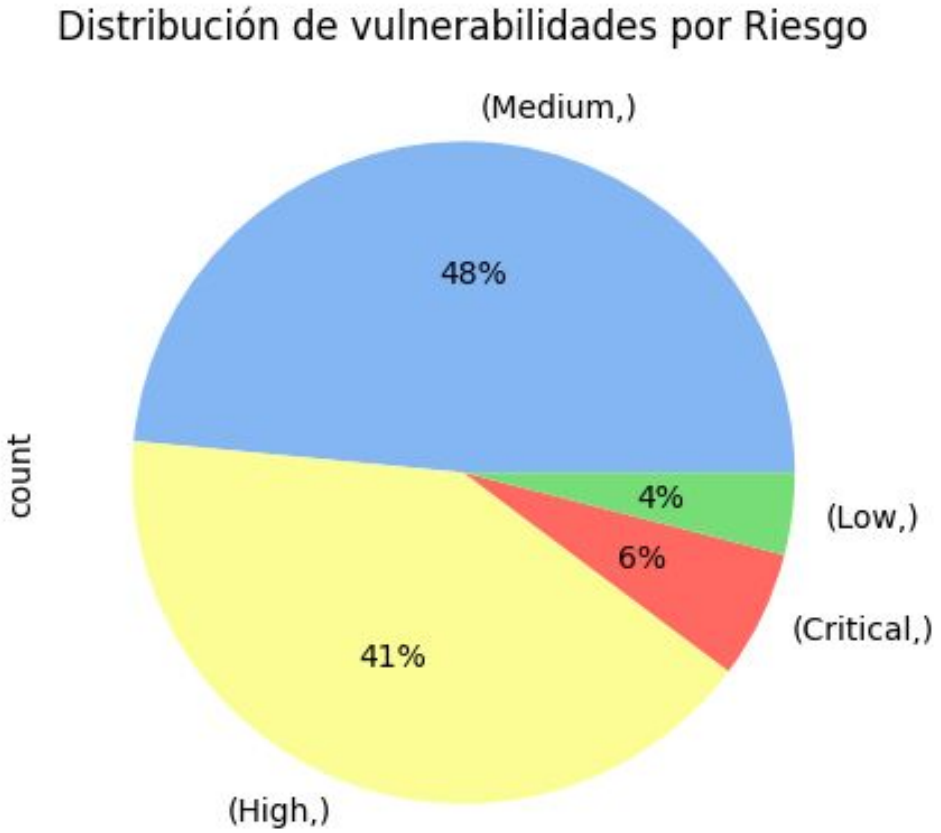


Equipos y sus vulnerabilidades

	Risk			
	count	unique	top	freq
Host				
192.168.170.164	182	4	High	84
192.168.170.204	7	3	Medium	3
192.168.170.211	33	4	Medium	23
192.168.170.213	180	4	High	84
192.168.170.228	178	4	High	83
192.168.170.91	17	4	Medium	11
192.168.170.99	28	4	Medium	22

Distribución de vulnerabilidades

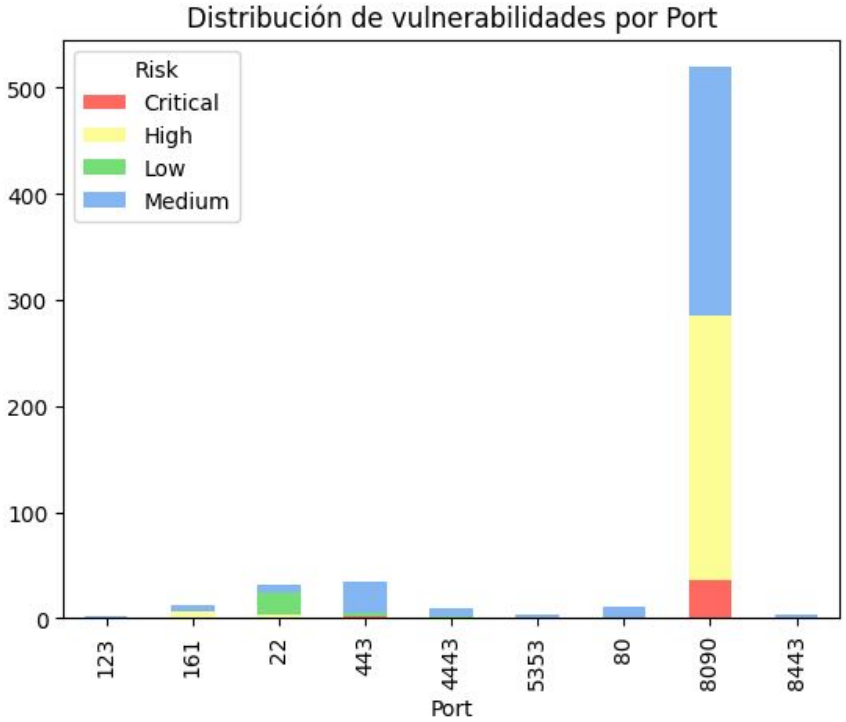
Riesgo	Cantidad
Crítico	39
Alta	258
Media	303
Baja	25
--------	-------
Total	625

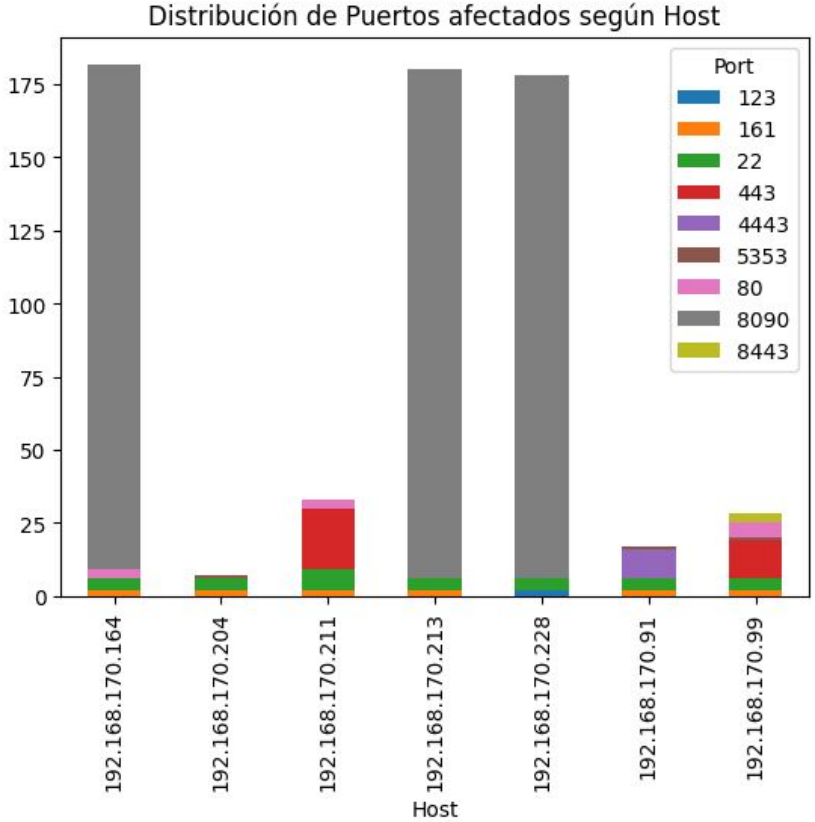


Distribución de vulnerabilidades

Host	Crítico	Alta	Media	
192.168.170.164	12	84	83	
192.168.170.213	12	84	81	
192.168.170.228	12	83	80	
Total	**36 (92,3%)**	**251 (97.3%)**	**244 (80,5%)**	**531 (~85%)**

Distribución de vulnerabilidades





¿Cual es el problema?

Las vulnerabilidades pueden ser explotadas lo cual llevaría a que la empresa pueda perder control del servicio, filtración de información, corrupción de los datos, entre otras.

Soluciones propuestas

Las principales soluciones a tener en cuenta para los equipos son las siguientes:

1. Actualizar OpenSSL a una versión más actual.
2. Actualizar Apache a una versión más actual.
3. Cambiar el nombre por defecto del servicio SNMP.
4. Deshabilitar métodos HTTP Trace y Track.
5. Actualizar versión PHP a una versión más actual.
6. En el servidor SSH deshabilitar CBC y habilitar CTR o GCM.

¿Por qué?

1. Con estas solucionan el mayor porcentaje de vulnerabilidades.
   a. **.218** = 175/180
   b. **.165** = 179/182
   c. **.228** = 173/178
2. Al actualizar los sistemas baja la posibilidad de un ataque cibernético.
3. Baja el impacto que pueda llegar a tener un ataque cibernético.

Para el futuro

Política de actualización de sistemas
En un determinado periodo de tiempo se debe estar al tanto de las correcciones, parches y actualizaciones de sistemas que lanzan los fabricantes de los programas utilizados e implementarlos lo antes posible.