Propuesta y análisis de ciberseguridad

4 de septiembre de 20XX

Descripción general

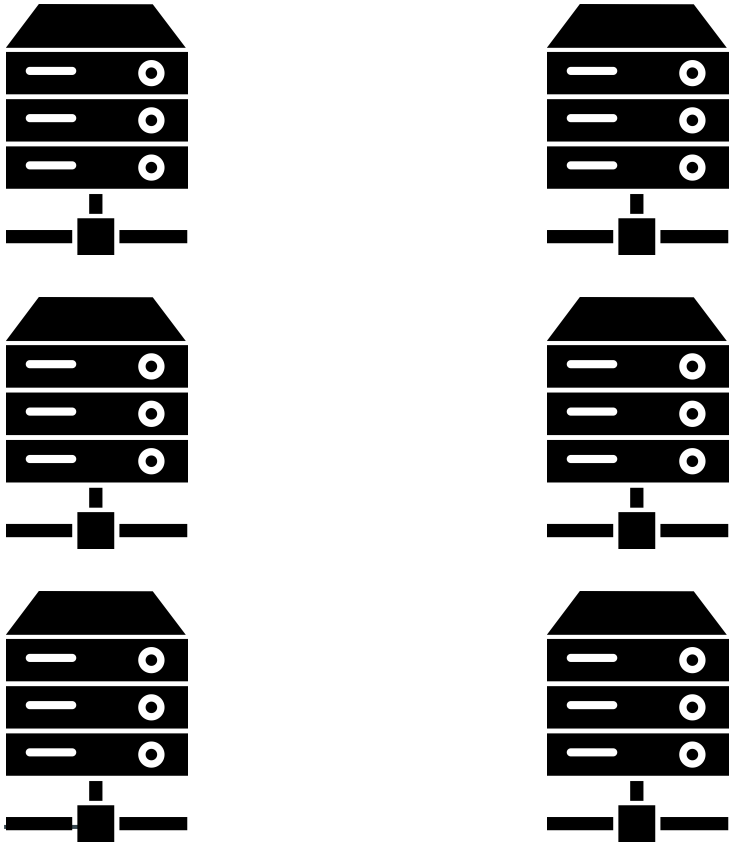
Se presenta análisis y propuesta solución de scan de vulnerabilidades para la empresa.

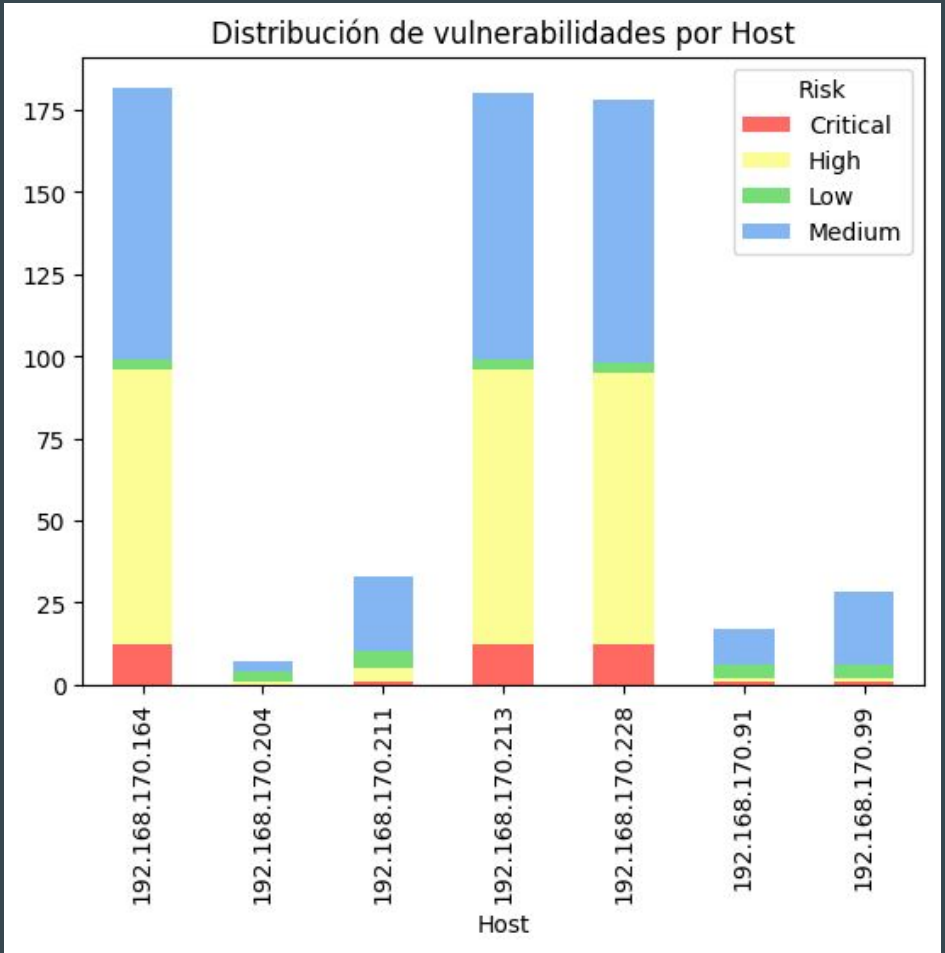
Objetivo del proyecto:

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



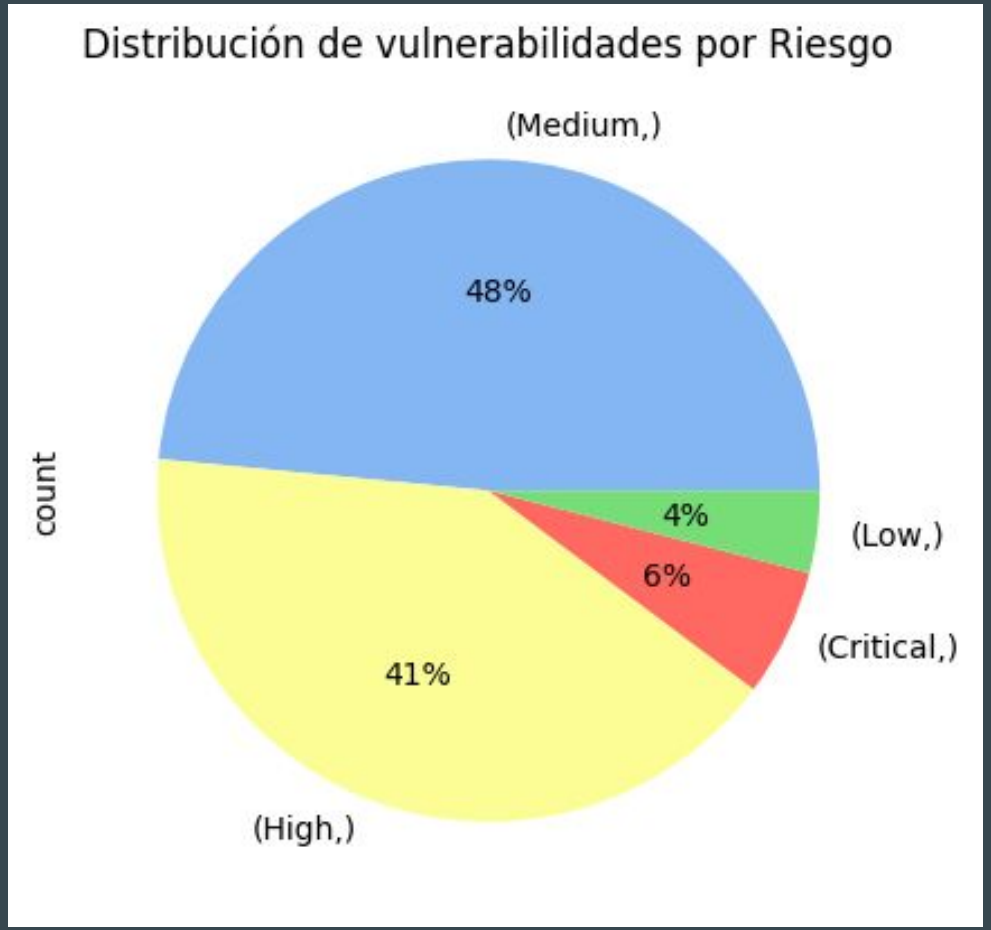


Equipos y sus vulnerabilidades

	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

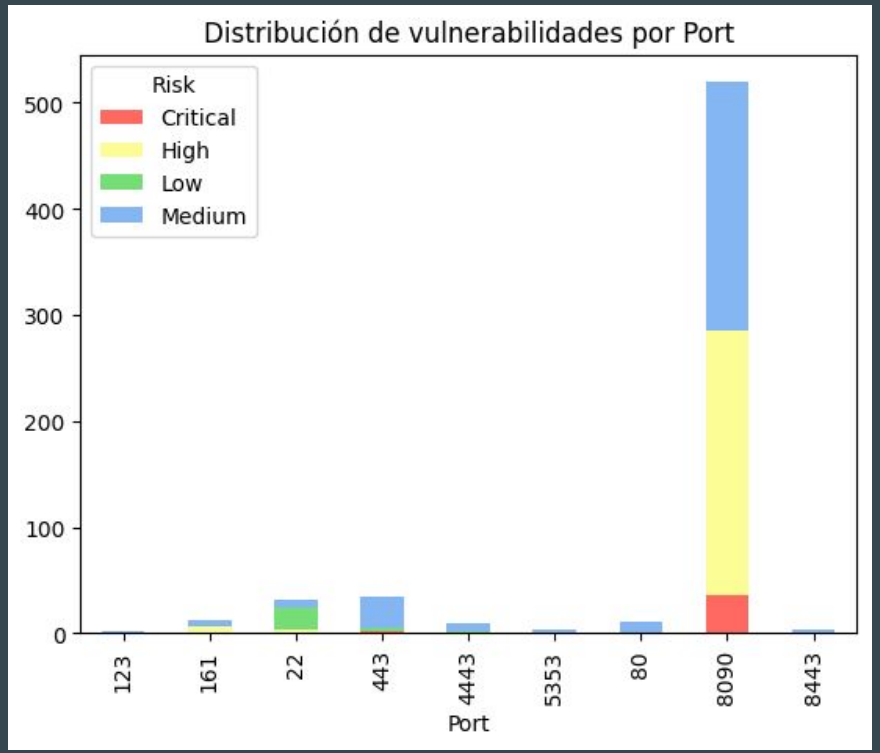
Riesgo	Cantidad
Crítico	39
Alta	258
Media	303
Baja	25
--------	-------
Total	625

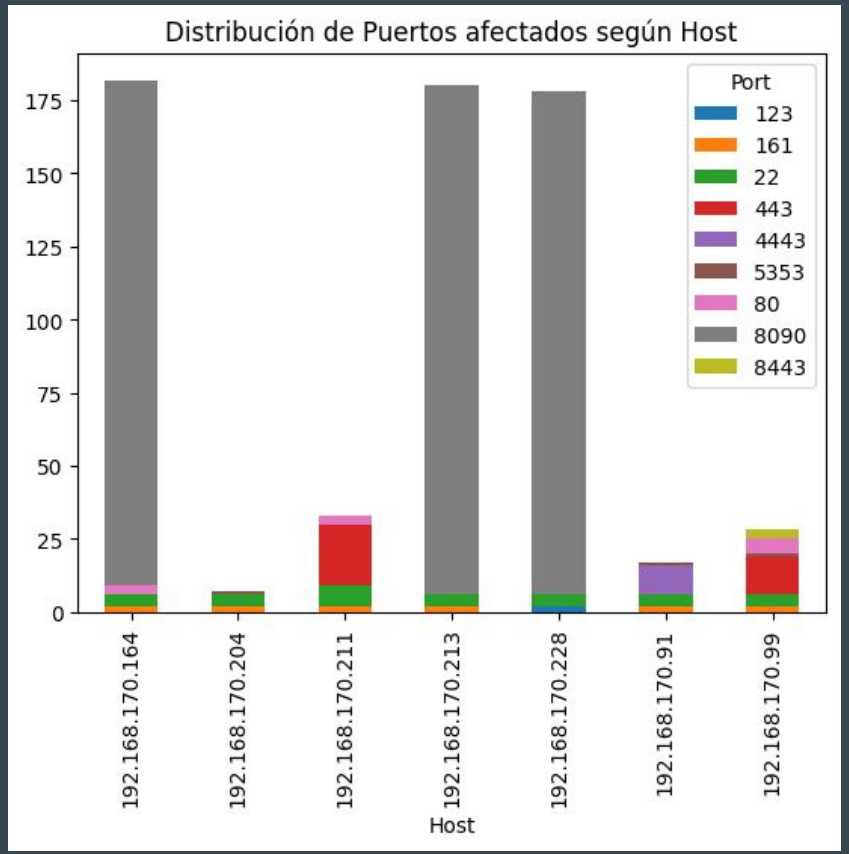


Distribución de vulnerabilidades

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





Soluciones propuestas

Para 192.168.70.213 y 192.168.70.164:

1. Cambiar el nombre por defecto del servicio SNMP, si no se está utlizando el servicio SNMP en el host remoto deshabilitarlo o si no, filtrar los paquetes UDP.
2. Actualizar OpenSSL a la versión mínima de 1.0.1s (La actual y recomendada es 3.2.1)
3. Actualizar Apache a la versión mínima de 2.4.47 (La actual y estable es 2.4.58)
4. Desabilitar métodos TRACE y TRACK de HTTP los cuales se utilizan para debuguiar y no deberían estar en producción.
5. Actualizar PHP a la versión mínima de 7.0.30 (La actual y recomendada es la 8.2 o 8.3)
6. En el servidor SSH deshabilitar CBC y habilitar CTR o GCM.

Esto debido a que la vulnerabilidad CVE-1999-0517 tiene un exploit conocido y la solución es bastante rápida. El resto del orden se mantiene igual ya que las actualizaciones son necesarias para poder eliminar la mayor cantidad de vulnerabilidades posibles, las cuales incluyen las críticas, altas y medias.

Para 192.168.70.228:

1. Actualizar OpenSSL a la versión mínima de 1.0.1s (La actual y recomendada es 3.2.1)
2. Actualizar Apache a la versión mínima de 2.4.47 (La actual y estable es 2.4.58)
3. Desabilitar métodos TRACE y TRACK de HTTP los cuales se utilizan para debuguiar y no deberían estar en producción.
4. Actualizar PHP a la versión mínima de 7.0.30 (La actual y recomendada es la 8.2 o 8.3)
5. En el servidor SSH deshabilitar CBC y habilitar CTR o GCM.

¿Por qué?

192.168.70.213	192.168.70.164	192.168.70.228
Este host tiene 180 vulnerabilidades de ellas: 74 que se solucionan con OpenSSL 72 que se solucionan con Apache 4 que se solucionan con HTTP 23 que se solucionan con PHP 2 que se solucionan con SNMP Por lo que con estas soluciones se resuelven 175/180	Este host tiene 182 vulnerabilidades de ellas: 74 que se solucionan con OpenSSL 73 que se solucionan con Apache 7 que se solucionan con HTTP 23 que se solucionan con PHP 2 que se solucionan con SNMP Por lo que con estas soluciones se resuelven 179/182	Este host tiene 178 vulnerabilidades de ellas: 74 que se solucionan con OpenSSL 72 que se solucionan con Apache 4 que se solucionan con HTTP 23 que se solucionan con PHP Por lo que con estas soluciones se resuelven 173/178

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.