Vulnerabilitats

https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/running-vu-scan.html

Per trobar les vulnerabilitats a les màquines cal configurar l'*ossec.conf* dels clients afegint les següents directrius:

```
<!-- Directives afegides per recollir les vulnerabilitats del sistema -->
 <wodle name="syscollector">
        <disabled>no</disabled>
        <interval>1h</interval>
        <os>yes</os>
        <packages>yes</packages>
        <hotfixes>yes</hotfixes>
 </wodle>
 <!-- Fi de les directives afegides -->
```

Nota: la línia *<hotfixes>yes</hotfixes>* és opcional i només per a màquines client Windows.

I al servidor Wazuh manager, cal tenir el fitxer */var/ossec/etc/ossec.conf* amb la directriu de detecció de vulnerabilitats a *yes*:

```
<vulnerability-detector>
 <enabled>yes</enabled>
```

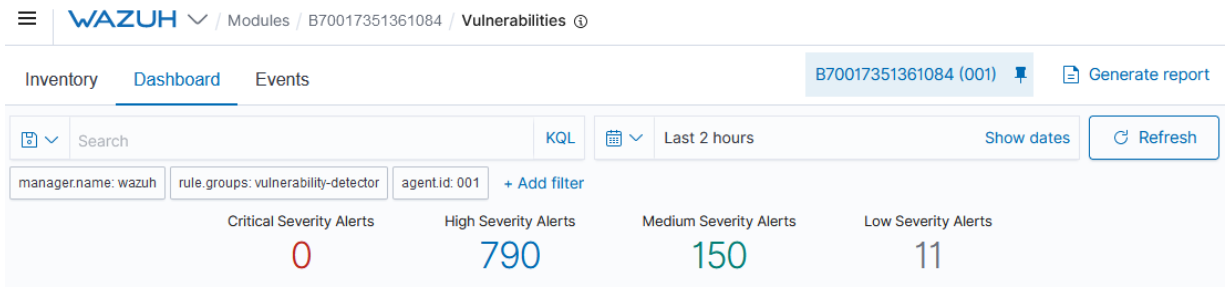
A més a més del tipus de clients linux, en el cas d'Ubuntu:

```
<vulnerability-detector>
 <enabled>yes</enabled>
 <interval>5m</interval>
 <ignore_time>6h</ignore_time>
 <run_on_start>yes</run_on_start>

 <provider name="canonical">
  <enabled>yes</enabled>
  <os>trusty</os>
  <os>xenial</os>
  <os>bionic</os>
  <os>focal</os>
  <update_interval>1h</update_interval>
 </provider>

 <provider name="debian">
  <enabled>no</enabled>
  <os>wheezy</os>
  <os>stretch</os>
  <os>jessie</os>
  <update_interval>1h</update_interval>
 </provider>

 <provider name="redhat">
  <enabled>no</enabled>
  <update_from_year>2010</update_from_year>
  <update_interval>1h</update_interval>
 </provider>
```

```
  <provider name="nvd">
    <enabled>yes</enabled>
    <update_from_year>2010</update_from_year>
    <update_interval>1h</update_interval>
  </provider>
</vulnerability-detector>
```

Un cop canviat cal reiniciar el servei.

Activitat: Cerca les vulnerabilitats de la teva màquina client i adjunta una captura la capçalera com aquesta on es vegi també el nom de la teva màquina:



Arregla totes les vulnerabilitats classificades com a *Critical Severity Alerts* i torna a adjuntar una captura amb aquest comptador a zero.

I si pots reduir la resta de vulnerabilitats tindràs millor nota!!!