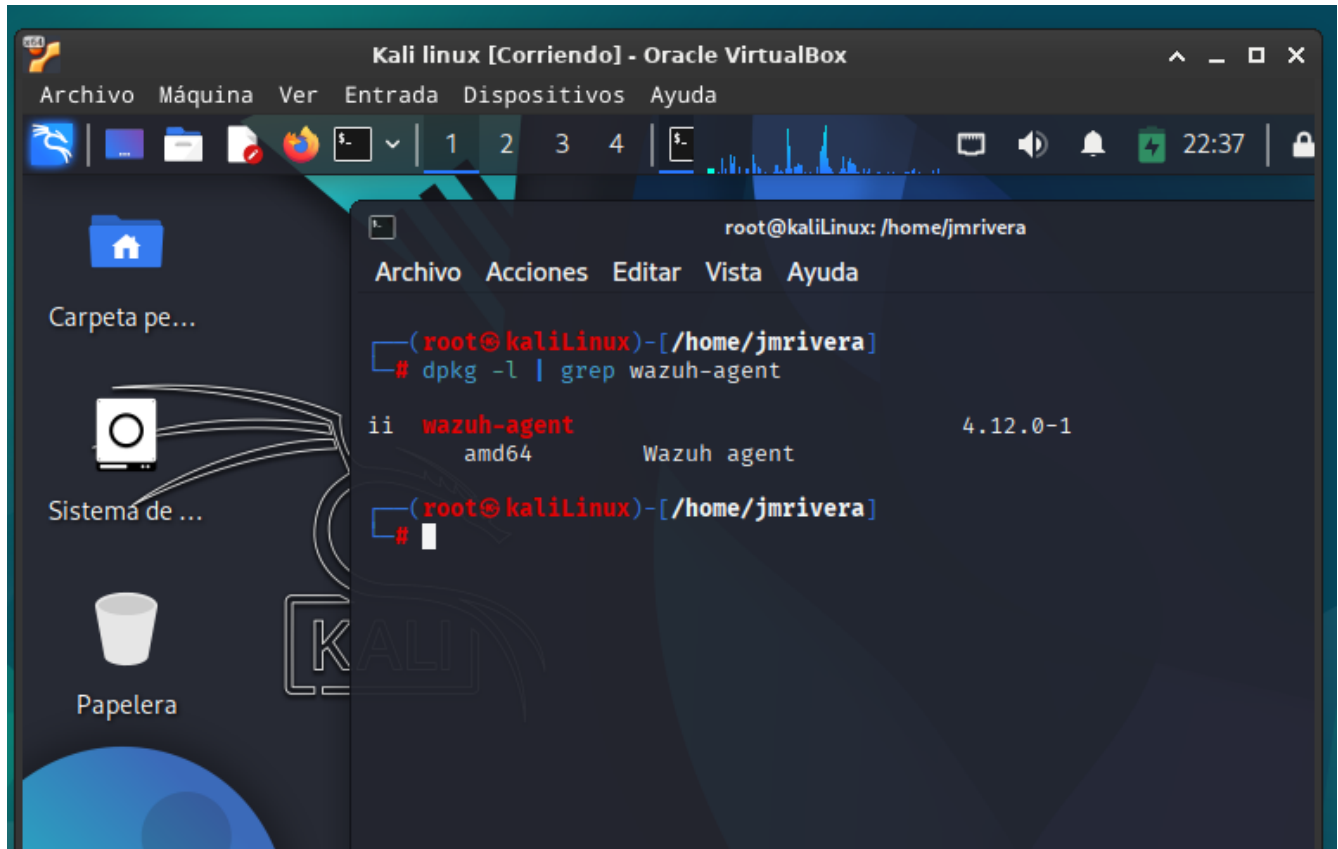


Desafío Prevención y detección de intrusiones
Seguridad en Redes de Datos
José Miguel Rivera

1. Generar la evidencia que demuestre la instalación de servidor WAZUH en servidor Kali Linux. (2 Puntos)



2. Generar evidencia que demuestre la instalación de agente WAZUH en equipo Windows. (2 Puntos)

Se realiza instalación de agente Wazuh en equipo Debian 12 usado como sistema anfitrión.

```
Terminal - jmriviera@debian12: ~
Archivo Editar Ver Terminal Pestañas Ayuda
jmriviera@debian12:~$ systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; preset: >
   Active: active (running) since Thu 2025-09-04 22:21:35 -04; 2min 34s ago
   Process: 15948 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (c>
   Tasks: 30 (limit: 14138)
   Memory: 161.5M
   CPU: 6.161s
   CGroup: /system.slice/wazuh-agent.service
           └─15972 /var/ossec/bin/wazuh-execd
             └─15985 /var/ossec/bin/wazuh-agentd
               └─15998 /var/ossec/bin/wazuh-syscheckd
                 └─16011 /var/ossec/bin/wazuh-logcollector
                   └─16028 /var/ossec/bin/wazuh-modulesd
lines 1-13/13 (END)
```

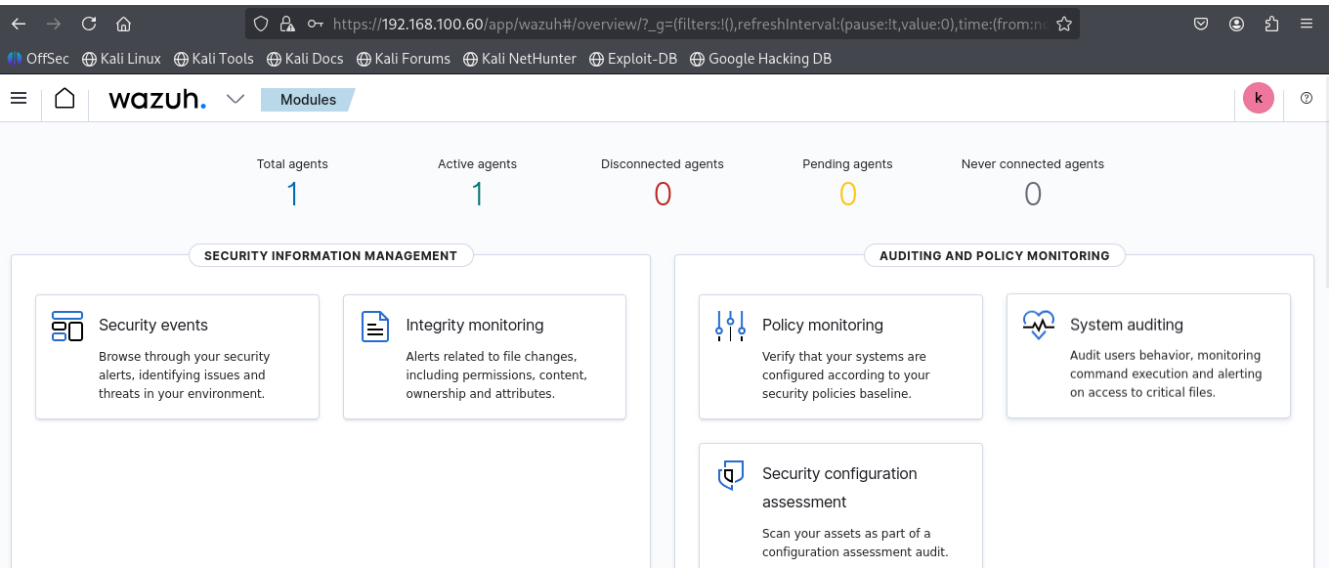
Se configura la IP local del servidor remoto Kali Linux 192.168.100.60

```
Terminal - jmriviera@debian12: ~
GNU nano 7.2 /var/ossec/etc/ossec.conf
<!--
Wazuh - Agent - Default configuration for debian 12
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

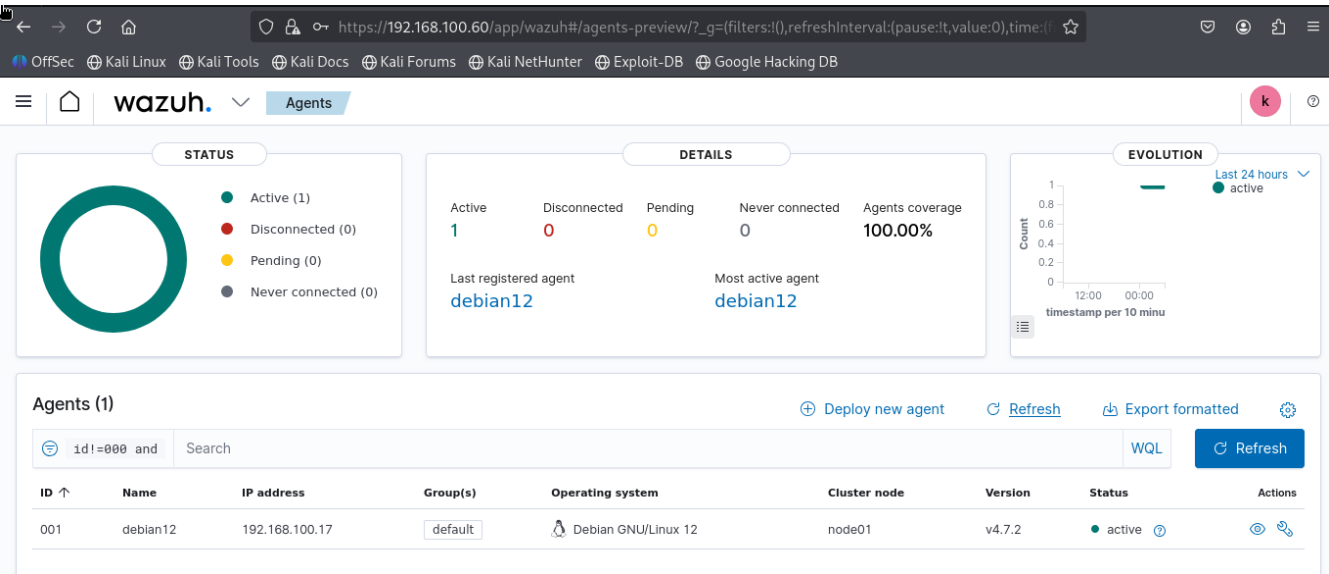
<ossec_config>
  <client>
    <server>
      <address>192.168.100.60
    </address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>debian, debian12</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>
[ 190 líneas leídas ]
^G Ayuda  ^O Guardar  ^W Buscar  ^K Cortar  ^T Ejecutar  ^C Ubicación
^X Salir  ^R Leer fich. ^\ Reemplazar ^U Pegar  ^J Justificar ^_ Ir a línea
```

3. Generar evidencia que demuestre la sincronización entre el agente WAZUH Windows y el servidor WAZUH en Kali Linux. (3 Puntos)

Dashboard de Wazuh validado el acceso



confirmación del agente debian12 (mi pc)



4. Generar evidencia de alertas que ha encontrado WAZUH en el equipo, muéstrelas y explique por qué la clasificación de la severidad. (3 Puntos)

Se verifican alertas por intentos de modificación de archivos importantes con clave de root, definido con valor 7 (importante)

OffSecKali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DB

wazuh

Modulesdebian12Security events

Security Alerts					
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Sep 8, 2025 @ 06:22:24.179			Host-based anomaly detection event (rootcheck).	7	510
> Sep 8, 2025 @ 06:22:23.121			Host-based anomaly detection event (rootcheck).	7	510
> Sep 8, 2025 @ 06:22:23.073			Host-based anomaly detection event (rootcheck).	7	510
> Sep 8, 2025 @ 06:20:33.152			Host-based anomaly detection event (rootcheck).	7	510
> Sep 8, 2025 @ 06:20:33.124			Host-based anomaly detection event (rootcheck).	7	510