Comandos Importantes para Pruebas Manuales en el Proyecto Wazuh

1. Ver estado de los agentes

```
/var/ossec/bin/agent_control -l
```

2. Forzar una alerta desde el cliente Windows

En el CMD del cliente:

```
net user prueba1 /add
```

3. Comprobar si llega la alerta al servidor

```
tail -f /var/ossec/logs/alerts/alerts.json
```

4. Enviar mensaje de prueba por Telegram (desde servidor)

```
curl -s -X POST https://api.telegram.org/bot<YOUR_BOT_TOKEN>/sendMessage -d chat_id=<CHAT_ID> -d text=" Alerta Wazuh: prueba de mensaje"
```

5. Enviar mensaje de prueba por Gmail (usando msmtp)

```
echo "Prueba de alerta por correo" | mail -s "Alerta Wazuh" tu-correo@gmail.com
```

6. Simular un evento desde log personalizado

```
echo "ERROR: Test de alerta generada manualmente" >> /var/ossec/logs/test.log
```

7. Probar Active Response

Telegram:

```
/var/ossec/active-response/bin/sendtelegram.sh    "Alerta generada manualmente desde script"
```

Gmail:

```
/var/ossec/active-response/bin/sendgmail.sh       "Alerta manual" "Este es un mensaje de prueba desde script"
```

8. Ver logs del sistema Wazuh

```
tail -n 50 /var/ossec/logs/ossec.log
```

9. Probar alertas desde wazuh-logtest

```
/var/ossec/bin/wazuh-logtest
```

Ejemplo dentro de wazuh-logtest:
Jun 20 12:00:00 servidor sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 22 ssh2