

# Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

## CryptoSEC: “*Careful where you step in*”



## Index

- **Descripció/Biografia:** -> readME <-
- **Practica:** -> readME <-
- **Bibliografia:** -> readME <-

## \_\_\_Wazuh\_\_\_

NOTA: S'ha intentat la instal·lació i configuració de Wazuh però ha donat molts problemes (*tried*)

## Descripció/Biografia

**Que es?** - Wazuh és un sistema de detecció d'intrusos en host de codi obert i lliure (HIDS).

- Wazuh és una solució de monitorització de seguretat gratuïta, de codi obert i llista per a empreses, monitorització d'integritat, resposta a incidents i

compliments.

- Wazuh és una plataforma Open Source utilitzada per a la prevenció, detecció i resposta a les amenaces.

### **Que fa?**

**Que pot fer?** - Realitza anàlisi de registre, comprovació d'integritat, supervisió del registre de Windows, detecció de rootkits, alertes basades en el temps i resposta activa.

- És capaç de protegir càrregues de treball en entorns locals, virtualitzats, en contenidors i al núvol.
- Wazuh aborda la necessitat de supervisió i resposta contínua a les amenaces avançades.
- Wazuh ajuda a detectar processos d'exploració ocults que són més complexos que un simple patró de signatura i que es poden utilitzar per evadir els sistemes antivirus tradicionals.
- Es pot utilitzar per monitoritzar punts finals, serveis al núvol i contenidors, i per afegir i analitzar dades de fonts externes.
- Proporciona detecció d'intrusions per a la majoria de sistemes operatius, incloent-hi Linux, AIX, HP-UX, macOS, Solaris i Windows.
- Wazuh té una arquitectura centralitzada i multiplataforma que permet que múltiples sistemes siguin fàcilment monitoritzats i administrats.
- Wazuh pot ser configurat per enviar alertes a syslog. Aquests missatges poden ser enviats a la interfície web de ServicePilot en temps real per syslog per a la seva anàlisi centralitzada.
- A més, l'agent de Wazuh proporciona capacitats de resposta activa que es poden utilitzar per bloquejar un atac de xarxa, detectar un procés maliciós o posar en quarantena un arxiu infectat amb codi maliciós (malware).

**Com ho fa?** - La solució Wazuh consta d'un agent de seguretat per a punts finals, desplegat als sistemes supervisats, i un servidor de gestió, que recull les dades de recopilades pels agents.

- Se centra a proporcionar la visibilitat adequada, amb els coneixements necessaris per ajudar les anàlisis de seguretat a descobrir, investigar i respondre a les amenaces i campanyes d'atac a diversos punts.

**Wazuh proporciona les capacitats següents:** - **Anàlisi de seguretat:** - Wazuh s'utilitza per recollir, llegir, agregar, indexar i analitzar dades de seguretat, ajudant les organitzacions a detectar intrusions, amenaces i comportaments anòmals dins de la xarxa.

- A mesures que les amenaces cibernètiques es tornen més sofisticades, es requereix de monitoratge en temps real i anàlisi de seguretat per a una

ràpida detecció i remediació de les amenaces.

- **Detecció d'intrusions:**

- Els agents de Wazuh analitza els sistemes monitoritzats buscant codi maliciós, rootkits i anomalies sospitoses. També poden detectar fitxers i processos ocults, ports de xarxa a l'escolta no registrat i inconsistències a les respostes a les trucades del sistema.
- A més d'aquestes capacitats dels agents, el servidor utilitza signatures per detectar intrusions, usant un motor d'expressions regulars per analitzar les dades dels logs.

- **Anàlisi de les dades de logs:**

- Als registres de sistemes, dispositius i aplicacions de la seva infraestructura, hi ha moltes situacions en què hi ha evidència d'atac. Wazuh es pot utilitzar per recopilar i analitzar dades de registre automàticament.
- Els agents de Wazuh llegeixen els logs de les aplicacions i del sistema operatiu i els envien de forma segura al servidor central per emmagatzemar-los i fer una anàlisi basada en regles. Aquestes regles ajuden a tenir coneixement d'errors del sistema o d'aplicació, errors de configuració, intents i/o èxit d'activitats malicioses, violacions de la política de seguretat i altres problemes d'operació o seguretat.

- **Monitorització de la integritat de fitxers:**

- Wazuh monitoritza el sistema de fitxers i identifica els canvis realitzats en el contingut, els permisos, la propietat i els atributs dels fitxers que han de vigilar. A més, identifica de forma nativa els usuaris i les aplicacions que s'utilitzen per crear o modificar fitxers.

- **Detecció de vulnerabilitats:**

- Els agents de Wazuh extreuen dades de l'inventari de programari i envien aquesta informació al servidor, on es correlaciona amb les bases de dades CVE (Common Vulnerabilities and Exposure) contínuament actualitzades, per identificar programari vulnerable conegut.
- L'avaluació de les vulnerabilitats de forma automàtica ens ajuda a trobar els punts vulnerables als actius crítics i prendre les accions correctives necessàries abans que siguin explotades pels atacants.

- **Avaluació de la configuració:**

- Wazuh ens ajuda a supervisar els ajustaments de configuració del sistema i les aplicacions per assegurar-nos que compleixi amb les polítiques de seguretat i estàndards.
- Els agents duen a terme escanejats periòdics per detectar les aplicacions que es coneix que són vulnerables, no aplicades o configurades

de forma insegura. A més, les revisions es poden personalitzar i fer a mida per adequar-se a la nostra organització.

- **Respostes a incidents:**

- Wazuh proporciona respostes activa llistes per ser utilitzades per tal de dur a terme diverses contramesures, com ara bloquejar accés a un sistema de l'origen de l'amenaça, per fer front a les amenaces.
- A més, Wazuh es pot utilitzar per executar ordres remotament o consultes al sistema, identificant indicadors de compromís (IOCs) i ajudant altres activitats forenses o tasques de resposta a incidents.

- **Compliment normatiu:**

- Wazuh proporciona alguns dels controls de seguretat necessaris per complir amb els estàndards i regulacions de la indústria.
- Wazuh es pot utilitzar per complir els requisits PCI DSS, GPG135 o GDPR6, utilitzant la seva interfície d'usuari web que proporciona informes i panells de control (dashboards) que ens poden ajudar a aquest compliment.

- **Monitorització de la seguretat:**

- Wazuh ajuda a la monitorització de la infraestructura al núvol de proveïdors com Amazon AWS, Azure o Google Cloud.
- A més, Wazuh proporciona regles per avaluar la configuració del seu entorn de núvol, detectant fàcilment les debilitats.

- **Seguretat en contenidors:**

- Wazuh proporciona visibilitat de seguretat als hosts i contenidors Docker, monitoritzant el seu comportament i detectant amenaces, vulnerabilitats i anomalies.
- L'agent de Wazuh té una integració nativa amb el motor Docker que permet als usuaris monitoritzar imatges, volums, configuracions de xarxa i contenidors en execució.

## **Practica: Instal·lar Wazuh Server a Ubuntu 20.04**

### **Instal·lar dependències**

```
sudo apt update
sudo apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common
```

### **Instal·lar Wazuh Manager**

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list
sudo apt update
```

```

sudo apt install wazuh-manager
sudo systemctl daemon-reload
sudo systemctl enable --now wazuh-manager
systemctl status wazuh-manager

```

### Instalar ELK Stack (Elasticsearch)

```

sudo apt install elasticsearch-oss opendistroforelasticsearch
curl -so /etc/elasticsearch/elasticsearch.yml https://raw.githubusercontent.com/wazuh/wazuh-
curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml https://
curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles_mapping.y
curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_users.y

sudo rm -f /etc/elasticsearch/{esnode-key.pem,esnode.pem,kirk-key.pem,kirk.pem,root-ca.pem}
sudo mkdir /etc/elasticsearch/certs && cd /etc/elasticsearch/certs
sudo curl -so ~/search-guard-tlstoool-1.8.zip https://maven.search-guard.com/search-guard-tlsto
sudo unzip ~/search-guard-tlstoool-1.8.zip -d ~/searchguard
sudo curl -so ~/searchguard/search-guard.yml https://raw.githubusercontent.com/wazuh/wazuh-
sudo ~/searchguard/tools/sgtlstoool.sh -c ~/searchguard/search-guard.yml -ca -crt -t /etc/ela
sudo rm /etc/elasticsearch/certs/client-certificates.readme
sudo systemctl enable --now elasticsearch
sudo /usr/share/elasticsearch/plugins/opendistro_security/tools/securityadmin.sh -cd /usr/sh
curl -XGET https://localhost:9200 -u admin:admin -k
sudo /usr/share/elasticsearch/bin/elasticsearch-plugin remove opendistro_performance_analyze

```

### Instalar Filebeat

```

sudo apt install filebeat
curl -so /etc/filebeat/filebeat.yml https://raw.githubusercontent.com/wazuh/wazuh-documentat
curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/4.1
chmod go+r /etc/filebeat/wazuh-template.json
sudo curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.1.tar.gz | tar -xvz -C
sudo mkdir /etc/filebeat/certs && cp /etc/elasticsearch/certs/root-ca.pem /etc/filebeat/certs/
sudo mv /etc/elasticsearch/certs/filebeat* /etc/filebeat/certs/
sudo systemctl enable --now filebeat
sudo filebeat test output
elasticsearch: https://127.0.0.1:9200...

```

### Instalar Kibana

```

sudo apt-get install opendistroforelasticsearch-kibana
curl -so /etc/kibana/kibana.yml https://raw.githubusercontent.com/wazuh/wazuh-documentation
sudo chown -R kibana:kibana /usr/share/kibana/optimize
sudo chown -R kibana:kibana /usr/share/kibana/plugins
cd /usr/share/kibana
sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/u
sudo mkdir /etc/kibana/certs

```

```

sudo cp /etc/elasticsearch/certs/root-ca.pem /etc/kibana/certs/
sudo mv /etc/elasticsearch/certs/kibana_http.key /etc/kibana/certs/kibana.key
sudo mv /etc/elasticsearch/certs/kibana_http.pem /etc/kibana/certs/kibana.pem
sudo setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node
sudo systemctl enable --now kibana
sudo ufw allow 443/tcp

```

```

URL: https://<wazuh_server_ip>
user: admin
password: admin

```

### Common errors

```

# curl https://raw.githubusercontent.com/wazuh/wazuh/v4.1.5/extensions/elasticsearch/7.x/wazuh-alerts-3.x-
# curl 'https://<kibana_ip>:<kibana_port>/api/saved_objects/index-pattern/wazuh-alerts-3.x-*'
# curl https://<ELASTICSEARCH_IP>:9200/_cat/indices/wazuh-alerts-* -u <elasticsearch_user>:<elasticsearch_password>
green open wazuh-alerts-4.x-2021.03.03 xwFPX7nFQxGy-05aBA3LFQ 3 0 340 0 672.6kb 672.6kb
filebeat test output
elasticsearch: https://127.0.0.1:9200...
parse url... OK
connection...
parse host... OK
dns lookup... OK
addresses: 127.0.0.1
dial up... OK
TLS...
security: server's certificate chain verification is enabled
handshake... OK
TLS version: TLSv1.3
dial up... OK
talk to server... OK
version: 7.10.0

```

### Bibliografia

**Deficions:** - <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/117787/7/jpcozarTFM0620memoria.pdf>  
 <– **GUIA PER A PROJECTE** - <https://blog.gudixsecurity.com/protege-tu-empresa-con-wazuh-edr-open-source/> - <https://www.servicepilot.com/es/integration/monitoreo-wazuh/> - <https://documentation.wazuh.com/current/index.html> - <https://es.wikipedia.org/wiki/Wazuh>

**Practica:** - <https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html>

- <https://www.csirt.gob.cl/media/2021/10/2SCSFP-SIEM-HE.pdf>
- <https://bobcares.com/blog/install-wazuh-server-on-ubuntu/>
- <https://www.youtube.com/watch?v=VLgmbv8a5O8>
- <https://gist.github.com/austinsonger/33c127fe4e760788b4ba3641295604fb>