



INSTALACION Y CONFIGURACION

SIEM

En el presente ejercicio se ha instalado la OVA de Wazuh 4.8.1, la cual una vez actualizada ha pasado a su versión 4.9.0, procediendo a su configuración para poder ser observada en su entorno GUI, en el navegador de mi Kali, configurando como agentes (NXlog) a la mencionada maquina y a la metaesplotable3, con la finalidad de recopilar y analizar los registros de datos de estos dispositivos, generándose alertas configuradas. Se ha seguido los siguientes pasos:

1. Se realiza las descarga, importación y actualización de la ova de Wazuh:

```
[root@wazuh-server ~]# /var/ossec/bin/wazuh-control info
WAZUH_VERSION="v4.9.0"
WAZUH_REVISION="40907"
WAZUH_TYPE="server"
```

2. Se configuran ambas maquinas en la mismas RED NAT para que exista comunicación entre ellas, siendo la termina en 5 la metaesplotable3 y la terminada en 15 el servidor de Wazuh:

```
kali@kali ~ [Local IP: 10.0.2.12] TARGET_IP: 10.0.2.15 % sudo arp-scan --localnet -I eth0
Linux wazuh-server 4.14.344-262.563.amzn2.x86_64 #1 SMP Fri May 17 18:07:48 UTC 2024
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:d2:26:79, IPv4: 10.0.2.12
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1 52:54:00:12:35:00 (Unknown: locally administered)
10.0.2.2 52:54:00:12:35:00 (Unknown: locally administered)
10.0.2.3 08:00:27:aa:aa:6b (Unknown)
10.0.2.5 08:00:27:f2:27:26 (Unknown)
10.0.2.15 08:00:27:db:7b:95 (Unknown)
```

3. Se conecta por ssh con la maquina Wazuh desde la Kali, para una mayor comodidad, conectando con el archivo principal de configuración de Wazuh, al cual se accede a través de "sudo nano /var/ossec/etc/ossef.conf", agregándole la IP del servidor de Wazuh.

```
<indexer>
<enabled>yes</enabled>
<hosts>
<host>https://10.0.2.15:9200</host>|
</hosts>
```

4. Se procede a comprobar los permisos de los certificados necesarios para la conexión SSL/TLS, ejecutando “`ls -ltr /etc/wazuh-indexer/certs`” y “`ls -ltr /etc/wazuh-dashboard/certs`” (certs, son las carpetas donde se guardan los certificados tanto del *módulo indexer y dashboard*), confirmando que no tienen los permisos necesarios, modificando los mismos “`chmod 644 /etc/wazuh-indexer/certs/*.pem`”:

```
[root@wazuh-server ~]# sudo chmod 600 /etc/wazuh-indexer/certs/*.pem
[root@wazuh-server ~]# ls -ltr /etc/wazuh-indexer/certs
total 20
-rw----- 1 wazuh-indexer wazuh-indexer 1229 Jun  6 17:53 wazuh-indexer.pem
-rw----- 1 wazuh-indexer wazuh-indexer 1708 Jun  6 17:53 wazuh-indexer-key.pem
-rw----- 1 wazuh-indexer wazuh-indexer 1184 Jun  6 17:53 root-ca.pem
-rw----- 1 wazuh-indexer wazuh-indexer 1107 Jun  6 17:53 admin.pem
-rw----- 1 wazuh-indexer wazuh-indexer 1704 Jun  6 17:53 admin-key.pem

[root@wazuh-server ~]# sudo chmod 644 /etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem
[root@wazuh-server ~]# sudo chmod 644 /etc/wazuh-dashboard/certs/root-ca.pem
[root@wazuh-server ~]# sudo chmod 644 /etc/wazuh-dashboard/certs/wazuh-dashboard.pem
[root@wazuh-server ~]# ls -ltr /etc/wazuh-dashboard/certs
total 12
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard 1184 Jun  6 17:53 root-ca.pem
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard 1233 Jun  6 17:53 wazuh-dashboard.pem
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard 1704 Jun  6 17:53 wazuh-dashboard-key.pem
[root@wazuh-server ~]#
```

5. Se accede al archivo de configuración del módulo Wazuh-Indexer, el cual se encuentra en “`etc/wazuh-indexer/opensearch.yml`”, donde se modifica el “`network.host`” con la dirección *IPV4*: 0.0.0.0, es decir para el que servidor pueda escuchar todas las interfaces, el “`http.port: 9200`”, así como el host y el puerto de transporte

El puerto 9200 es usado por Wazuh-indexer (similar al opensearch) para consultas externas, siendo un puerto fundamental para las comunicaciones de las aplicaciones externas (dashboard, API, etc...) con su motor de búsqueda, donde se almacenan los logs y eventos de seguridad, es decir, es el puerto a través del que se realizan las consultas de datos con los datos almacenados en Wazuh-Indexer.

```
#escucha todos las interfaces
network.host: 0.0.0.0
#puerto predeterminado
http.port: 9200
#Ip del servidor de WAZUH
transport.host: 10.0.2.15
#Puertos para el transporte
transport.port: 9300-9400
```

Por otro lado, el host y puerto de transporte de Wazuh-Indexer, son necesarios para configurar la comunicación interna entre los diferentes nodos de Wazuh-Indexer, siendo éste, el componente básico de Wazuh que ejecuta tareas de almacenamiento. Además, garantizan la correcta operación del/los clústeres/s, los cuales están formados por un conjunto de nodos que trabajan juntos en la gestión de grandes volúmenes de datos dentro de Wazuh.

- Se accede al archivo de configuración de Wazuh-dashboard, accediendo a través de la ruta “`etc/wazuh-dashboard/opensearch_dashboards.yml`”, estableciendo el `server.host` para que el dashboard pueda escuchar cualquier IP y el puerto que utilizará para la conexión la interfaz GUI del dashboard a través del navegador (se puede establecer otro puerto).

```
server.host: "0.0.0.0" # Permite que Wazuh Dashboard escuche en todas las interfaces.
server.port: 5601 # Puerto para acceder al Dashboard.
# Configuración del Indexer (Wazuh Indexer o OpenSearch)
opensearch.hosts: ["https://10.0.2.15:9200"] # La IP y el puerto de tu Wazuh Indexer
```

También se establece el `hosts` para la comunicación interna entre Wazuh-dashboard y Wazuh-indexer, como se explicó anteriormente.

- Una vez acabada la configuración se restauran los tres módulos de Wazuh y se comprueba sus estados, estando todos en perfecto funcionamiento.

```
[root@wazuh-server ~]# sudo systemctl restart wazuh-manager
[root@wazuh-server ~]# sudo systemctl restart wazuh-indexer
[root@wazuh-server ~]# sudo systemctl restart wazuh-dashboard
[root@wazuh-server ~]# sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2024-09-15 11:31:33 UTC; 1min 2s ago
     Process: 24139 ExecStop=/usr/bin/env /var/ossec/bin/wazuh-control stop (code=exited, status=0/SUCCESS)
    Process: 24272 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
[root@wazuh-server ~]# sudo systemctl status wazuh-indexer
● wazuh-indexer.service - wazuh-indexer
   Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2024-09-15 11:31:46 UTC; 50s ago
     Docs: https://documentation.wazuh.com
    Main PID: 25118 (java)
    CGroup: /system.slice/wazuh-indexer.service
            └─25118 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60
● wazuh-dashboard.service - wazuh-dashboard
   Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2024-09-15 11:31:46 UTC; 50s ago
    Main PID: 25454 (node)
    CGroup: /system.slice/wazuh-dashboard.service
            └─25454 /usr/share/wazuh-dashboard/node/fallback/bin/node /usr/share/wazuh-dashboard/src/cli/dist
```

- Se procede a comprobar la interfaz GUI a través del navegador de la Kali, a través de la [URL:https://10.0.2.15:5601](https://10.0.2.15:5601), siendo resultado positivo, pero aun no habiendo ningún agente instalado.



9. Una vez acabado con el servidor de Wazuh, ahora se van a configurar los “Wazuh-agents” para la Kali y para la Metasploitable 3, llevando a cabo las siguientes acciones en cada una de las maquinas:

- Descarga e Instalación:

```
kali@kali ~/Downloads [Local IP: 10.0.2.12] TARGET_IP: 10.0.2.5 % sudo dpkg -i wazuh-agent_4.9.0-1_amd64.deb
[sudo] password for kali:
Selecting previously unselected package wazuh-agent.
(Reading database ... 470797 files and directories currently installed.)
Preparing to unpack wazuh-agent_4.9.0-1_amd64.deb ...
Unpacking wazuh-agent (4.9.0-1) ...
Setting up wazuh-agent (4.9.0-1) ...
```

```
VBoxGuestAdditions.iso wazuh-agent_4.9.0-1_amd64.deb
vagrant@metasploitable3-ub1404:~$ sudo dpkg -i wazuh-agent_4.9.0-1_amd64.deb
(Reading database ... 99239 files and directories currently installed.)
Preparing to unpack wazuh-agent_4.9.0-1_amd64.deb ...
Unpacking wazuh-agent (4.9.0-1) over (4.9.0-1) ...
Setting up wazuh-agent (4.9.0-1) ...
Processing triggers for ureadahead (0.100.0-16) ...
```

- Activación de la Key para cada agente, siendo una credencial única que genera la API de Wazuh para la autenticación de nuevos dispositivos (Kali y metasploitable3):

```
# sudo /var/ossec/bin/agent-auth -m 10.0.2.15 -A kali wazuh-agent_4.9.0-1_amd64.deb
sudo: dpkg: command not found
2024/09/15 14:43:57 agent-auth: INFO: Started (pid: 18411).
2024/09/15 14:43:57 agent-auth: INFO: Requesting a key from server: 10.0.2.15
2024/09/15 14:43:57 agent-auth: INFO: No authentication password provided
2024/09/15 14:43:57 agent-auth: INFO: Using agent name as: kali
2024/09/15 14:43:57 agent-auth: INFO: Waiting for server reply
2024/09/15 14:43:57 agent-auth: INFO: Valid key received
Setting up wazuh-agent (4.9.0-1) ...
```

```
vagrant@metasploitable3-ub1404:~$ sudo /var/ossec/bin/agent-auth -m 10.0.2.15 -A metasploitable3
2024/09/15 12:34:29 agent-auth: INFO: Started (pid: 7423).
2024/09/15 12:34:29 agent-auth: INFO: Requesting a key from server: 10.0.2.15
2024/09/15 12:34:29 agent-auth: INFO: No authentication password provided
2024/09/15 12:34:29 agent-auth: INFO: Using agent name as: metasploitable3
2024/09/15 12:34:29 agent-auth: INFO: Waiting for server reply
2024/09/15 12:34:29 agent-auth: INFO: Valid key received
```

Con el comando “`sudo /etc/ossec/bin/agent-auth -m xxx -A xxx`”, es la manera de agregar manualmente a un nuevo agente en el Wazuh-manager, usando la ruta completa para ejecutar el comando “`agent-auth`” (no incluida en el PATH del sistema), el cual se encarga de autenticar al nuevo agente, y las opciones -m y -A, es usan para déficit la IP del servidor Wazuh-manager y dar el nombre al nuevo agente, respectivamente.

- Configuración de los Wazuh-agents en sus archivos sitos en `“/var/ossec/etc/ossef.conf”`, cambiando el campo `“MANAGER_IP”` por la IP de nuestro servidor `:10.0.2.15`, dentro de los tags `“address”`:

```
GNU nano 2.8.1 /var/ossec/etc/
-- editing database ... 99239 files and directories currently installed.)
Wazuh - Agent - Default configuration for kali 2024.3
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
--> cessing triggers for ureadah...
agrant@metasploitable3-ub14.04.13 report
<ossec_config> be root
<client> metasploitable3-ub14.04.13
<server> metasploitable3-ub14.04.13
<address>10.0.2.15</address>
<port>1514</port>
GNU nano 2.2.6 File: /var/ossec/etc/ossec.conf
```

- Restauración y comprobación:

```

# sudo systemctl restart wazuh-agent
2024/09/15 12:34:29 agent-auth: INFO: Requested a key from server 30.0.2.15
2024/09/15 12:34:29 agent-auth: INFO: Requested a key from server 30.0.2.15
(root@kali) [/usr/share/lintian/overrides] and the password provided
# sudo systemctl status wazuh-agent
Active: active (running) since Sun 2024-09-15 14:52:28 CEST; 6s ago
Invocation: b8a503f23a024726be475a160a9c04f7
Process: 22711 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
Tasks: 31 (limit: 9437)
vagrant@metasploitable3-ub1404:~$ sudo systemctl restart wazuh-agent
sudo: systemctl: command not found
vagrant@metasploitable3-ub1404:~$ #el comando no esta version de ubuntu
vagrant@metasploitable3-ub1404:~$ sudo ls /var/ossec/bin
agent-auth manage_agents wazuh-agentd wazuh-control wazuh-execd wazuh-logcollector
vagrant@metasploitable3-ub1404:~$ sudo /var/ossec/bin/wazuh-control start
Starting Wazuh v4.9.0...
Started wazuh-execd...
Started wazuh-agentd...
Started wazuh-syscheckd...
Started wazuh-logcollector...
Started wazuh-modulesd...
Completed.
vagrant@metasploitable3-ub1404:~$ sudo /var/ossec/bin/wazuh-control start
Starting Wazuh v4.9.0...
wazuh-execd already running...
wazuh-agentd already running...
wazuh-syscheckd already running...
wazuh-logcollector already running...
wazuh-modulesd already running...
Completed.
vagrant@metasploitable3-ub1404:~$ sudo /var/ossec/bin/wazuh-control status
wazuh-modulesd is running

```

10. Resultado final de todas las operaciones, es la correcta instalación y configuración predeterminada con dos agentes Wazuh (Kali y metaexploitable3):

```
*****
* Wazuh v4.9.0 Agent manager.      *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: l

Available agents:
ID: 003, Name: metaexploitable3, IP: any
ID: 004, Name: kali, IP: any
```

