



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE CIENCIAS

### Práctica 07: Lookout, guardian, sentry - Las Canijas Lagartijas

#### ALUMNOS

Gabriela López Diego - 318243485

Abraham Jiménez Reyes - 318230577

Javier Alejandro Rivera Zavala - 311288876

Juan Daniel San Martín Macías - 318181637

#### PROFESORA

Anayansi Delia Martínez Hernández

#### AYUDANTES

Cecilia del Carmen Villatoro Ramos

Roberto Adrián Bonilla Ruiz

Ivan Daniel Galindo Perez

Roberto Adrián Bonilla Ruiz

#### ASIGNATURA

Criptografía y Seguridad

Fecha de entrega: 17 de Abril del 2024

# 1. Introducción

Ésta práctica tiene como objetivo poner a prueba un malware (ransomware y spyware), al conectar dos endpoints a un sistema SIEM (Security Information and Event Management) o EDR (Endpoint Detection and Response). El propósito es observar cómo se generan las alertas antes y después de los ataques realizados con el malware. En este caso, utilizaremos Wazuh como la solución SIEM/EDR para monitorear las actividades en los endpoints.

Wazuh es una plataforma de código abierto que ofrece capacidades avanzadas de detección y respuesta a incidentes a nivel de endpoints. Al conectar los endpoints a Wazuh, podremos observar en tiempo real cómo el malware interactúa con el entorno y cómo el sistema de seguridad responde a las actividades maliciosas.

# 2. Desarrollo

Comenzaremos por instalar Wazuh desde su pagina principal <https://www.wazuh.com/>

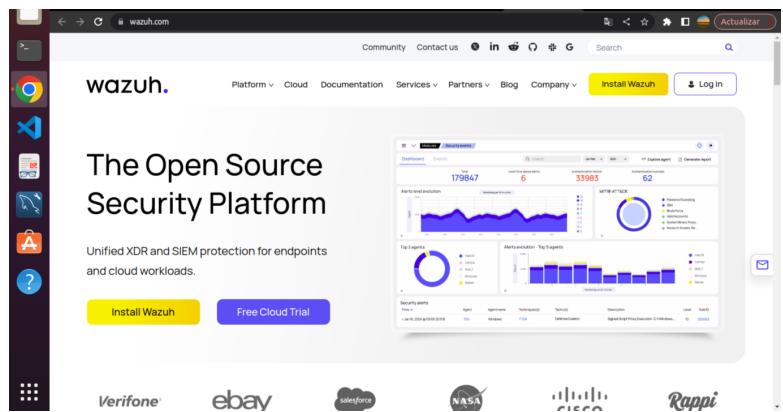


Figura 1: Pagina oficial de Wazuh

Nos daran el siguiente comando para iniciar con la instalacionm se instalaran las dependencias; wazuh-manager, wazuh-dashboard, wazuh-indexer;

```
curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

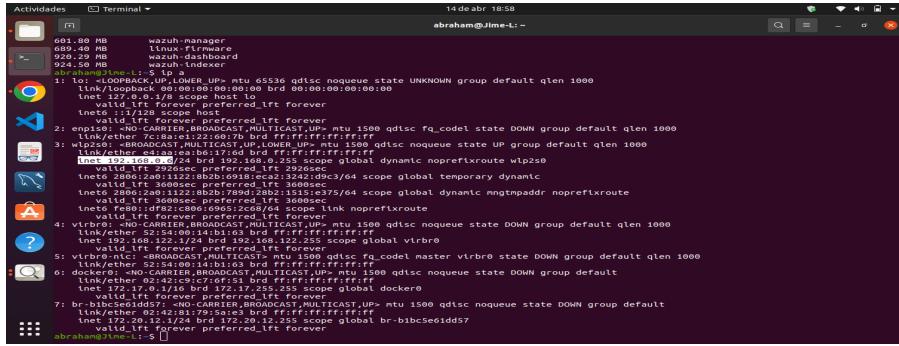
Si todo sale bien deberia verse de la siguiente manera

A screenshot of a terminal window on a Linux system. The title bar says 'Actividades Terminal' and the date is '14 abr 15:19'. The user is 'abraham@JLme-Li-'. The terminal shows a log of the installation process for Wazuh components: Wazuh Manager, Wazuh Dashboard, and Filebeat. The log includes messages like 'INFO: Wazuh web interface port will be 443.', 'INFO: Wazuh repository added.', 'INFO: Configuration files created.', 'INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for instal...', and 'INFO: Wazuh indexer ... Starting Wazuh Under installation... Installation finished.' The terminal ends with '14/04/2024 14:25:12 INFO: User: admin'. The bottom of the terminal shows the command 'curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a'.

Figura 2: Terminal que muestra que la instalación fue correcta

En la imagen tenemos nuestro user y password para poder iniciar sesion.

Ahora solo necesitamos saber nuestra ip y pegarla con el puerto 443.



```
Actuviades Terminal abraham@Jlime-Li ~
14 de abr 18:58

abraham@Jlime-Li ~
[abraham@Jlime-Li ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 6536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
2: ens1f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 7c:8a:1e:12:21:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.6 brd 192.168.0.255 scope global dynamic noprefixroute wlp2s0
        valid_lft 292256sec preferred_lft 292256sec
    link/ether 04:aa:ea:be:b1:03 brd ff:ff:ff:ff:ff:ff
        valid_lft 292256sec preferred_lft 292256sec
    link/ether 02:42:c9:c7:0f:51 brd ff:ff:ff:ff:ff:ff
        valid_lft forever preferred_lft forever
3: vrtbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 02:42:c9:c7:0f:51 brd ff:ff:ff:ff:ff:ff
    inet 172.20.12.1/24 brd 172.20.12.255 scope global docker0
        valid_lft forever preferred_lft forever
4: vrtbr0:1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 02:42:c9:c7:0f:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global vrtbr0
        valid_lft forever preferred_lft forever
5: vrtbr0:2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:14:b1:03 brd ff:ff:ff:ff:ff:ff
    inet 172.20.12.2/24 brd 172.20.12.255 scope global br-bbce61dd57
        valid_lft forever preferred_lft forever
[abraham@Jlime-Li ~]$
```

Figura 3: Terminal que muestra nuestras direcciones ip

En el buscador solo ponemos <https://192.168.0.6:443> y nos aparecerá Wazuh.

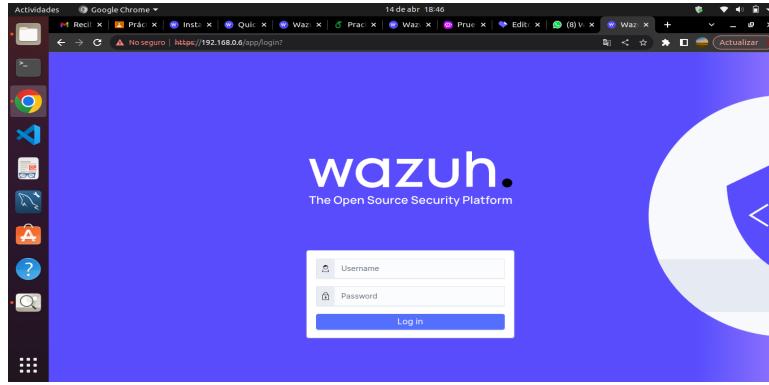


Figura 4: Ventana de inicio de Wazuh

Ya que ingresamos nuestro usuario y contraseña entraremos al panel principal de Wazuh

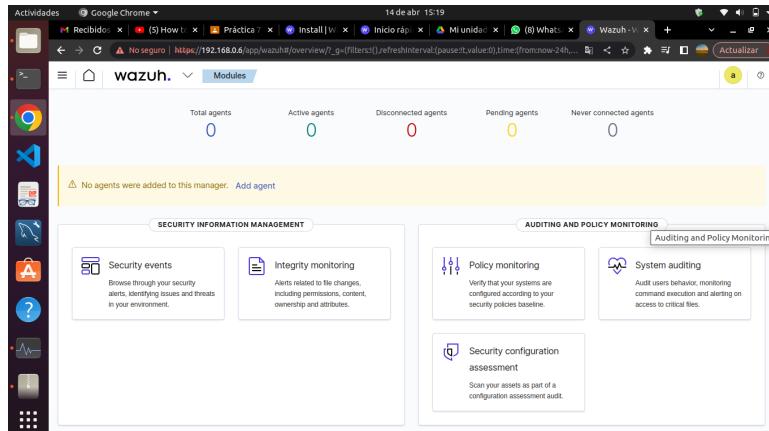


Figura 5: Panel de dashboard

Cuando tengamos la instalación se vera de la siguiente manera:

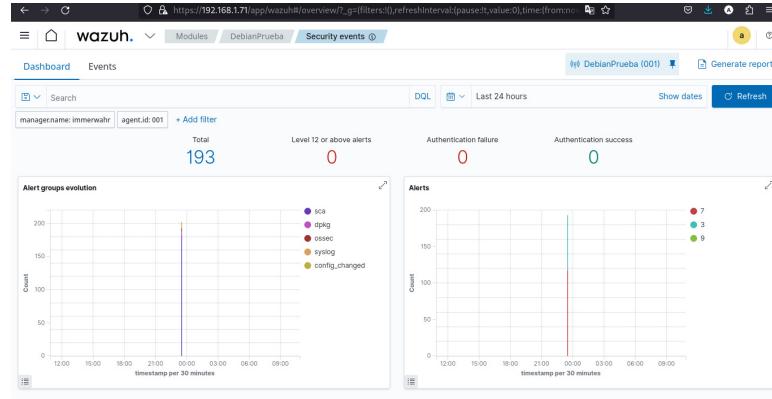


Figura 6: Panel de dashboard

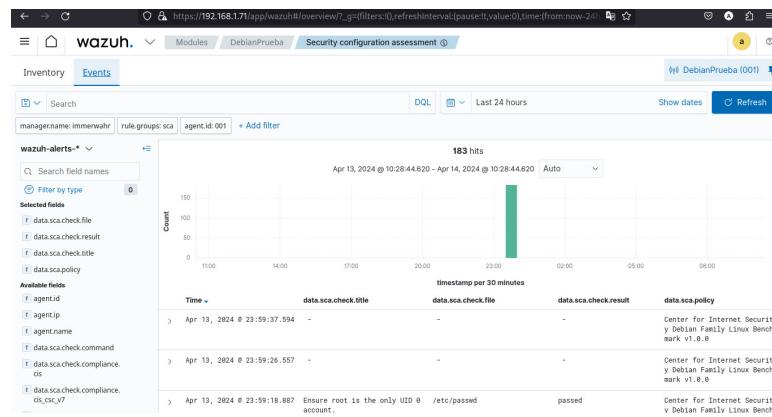


Figura 7: Panel de eventos

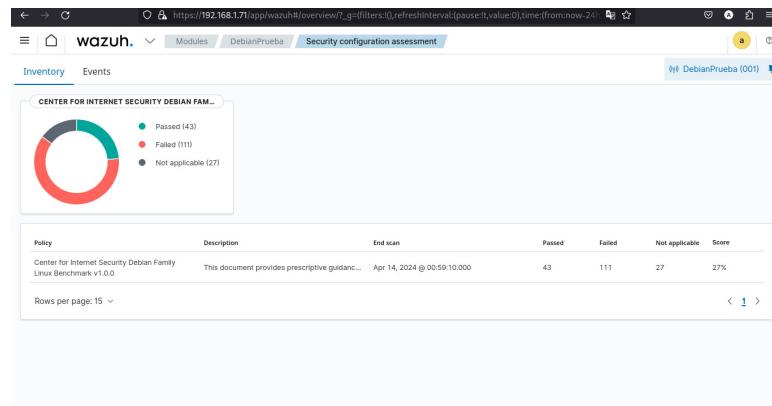


Figura 8: Panel de inventory

Luego, para poder instalar un agente en la maquina virtual que contiene el sistema operativo windows 10, seguiremos las instrucciones de wazuh agent <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>. Primero descargamos *Windows installer*, luego lo colocamos dentro de una carpeta con nombre *wazuh* dentro del disco local C de la MV con windows 10. Una vez hecho lo anterior nos dirigimos de regreso a nuestro sistema operativo principal linux y en la página principal de wazuh (Figura 5), damos click en **Add agent** el cual nos muestra lo siguiente

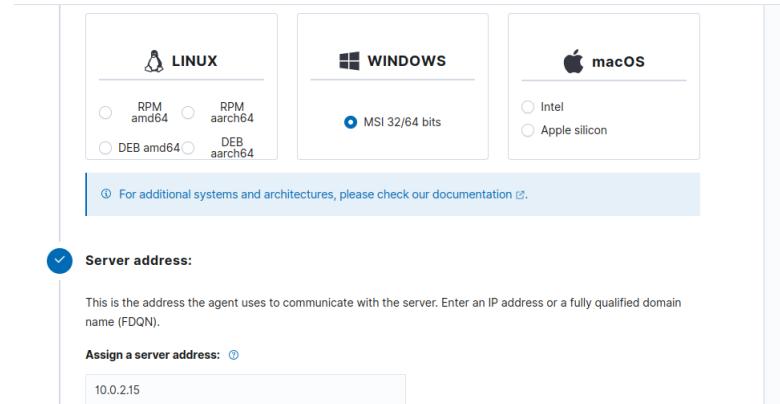


Figura 9: Creación del agente para windows 10

Seleccionamos la opción de windows ya que es el sistema operativo que deseamos monitorear, al igual que la IP de nuestro sistema principal linux (en este caso **192.168.0.104**), le asignamos un nombre al agente **agentcripto** y se nos genera el siguiente comando listo para ejecutar en windows 10 y poder descargar el agente en la MV.

```
1 Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile ${env.tmp}\wazuh-agent; msieexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.0.104' WAZUH_AGENT_NAME='agentcripto' WAZUH_REGISTRATION_SERVER='192.168.0.104'
```

Regresamos a nuestra MV con windows 10 y abrimos powershell con permisos de administrador. Nos dirigimos a la carpeta que contiene *windows installer* y ejecutamos el siguiente comando

```
1 .\wazuh-agent-4.7.3-1.msi /q WAZUH_MANAGER="10.0.2.15"
```

Donde 10.0.2.15 es el IP de la MV con windows 10. Una vez realizado lo anterior, procedemos a ejecutar el comando anterior generado, tal como se muestra a continuación

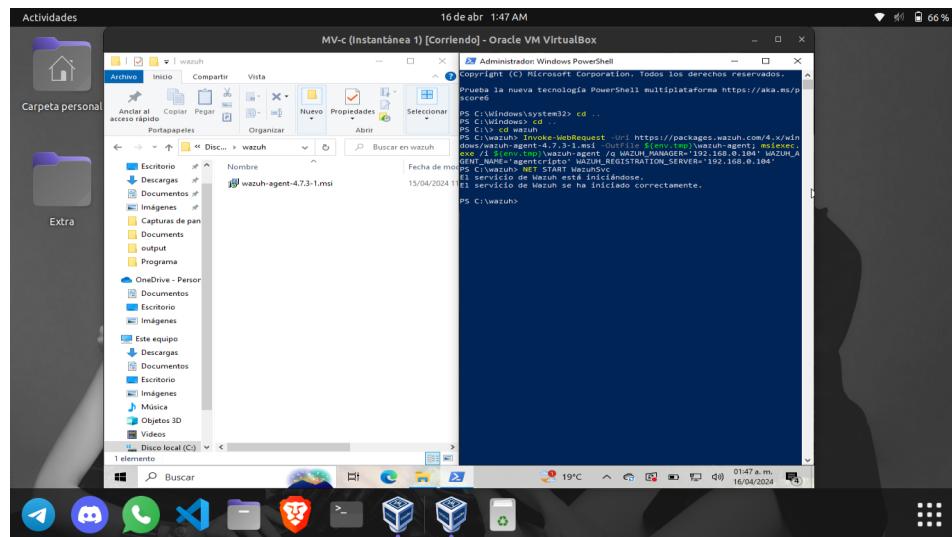


Figura 10: Instalación del agente agentcripto

Después, con el comando NET START Wazuh logramos observar que de forma exitosa comenzamos a monitorear el equipo ya que si regresamos a wazuh con el ip de nuestro equipo principal, *agentcripto* se encuentra registrado como nuevo agente.

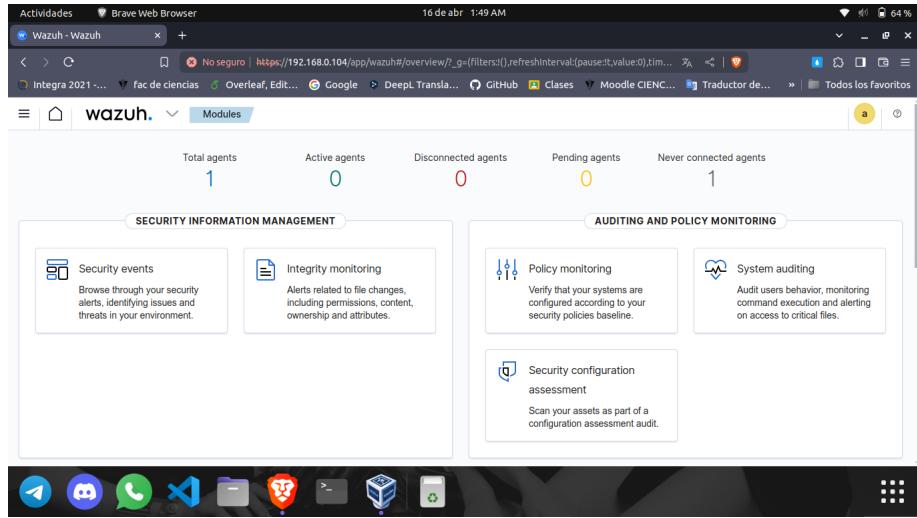


Figura 11: Wazuh y el nuevo agente agregado

Los datos recolectados, avisos y alertas sobre amenazas en el equipo ANTES de la ejecución del *Ransomware* son los siguientes

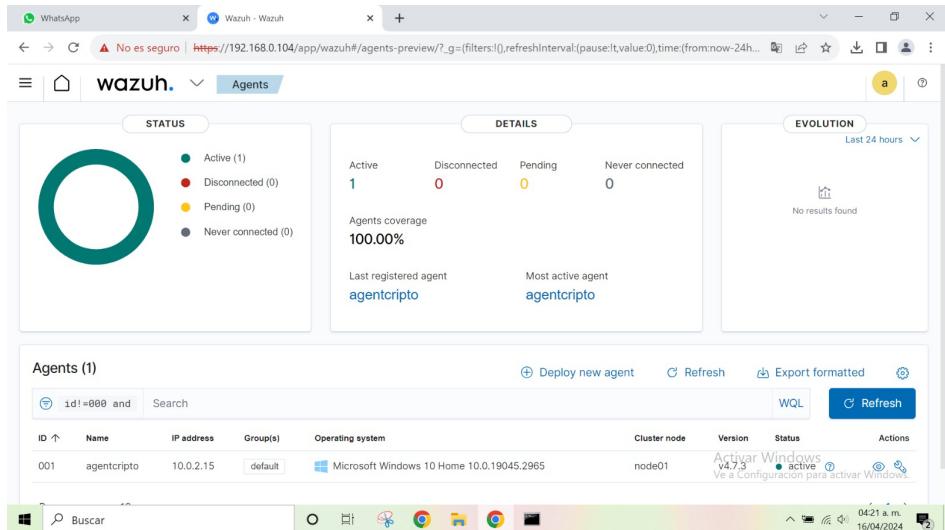


Figura 12: Tablero estatus

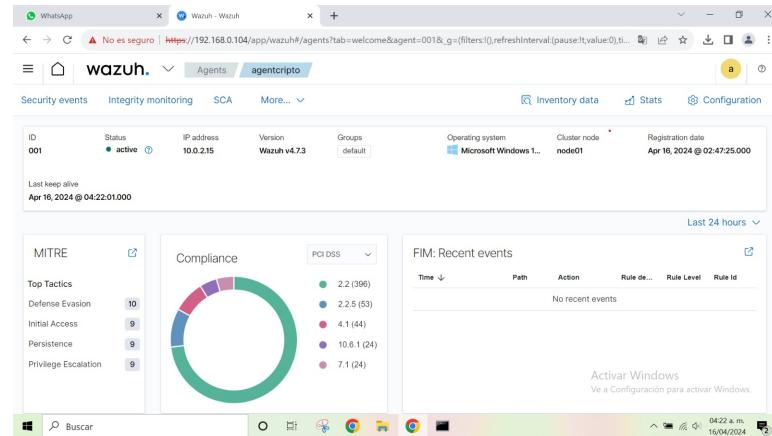


Figura 13: Datos recopilados ANTES del ransomware

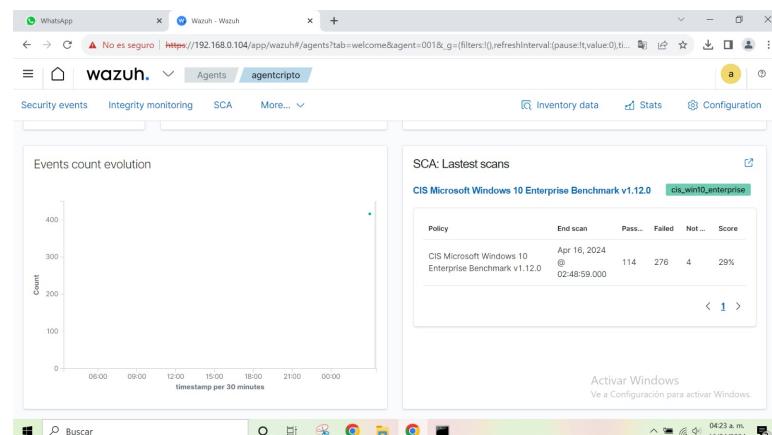


Figura 14: Datos recopilados ANTES del ransomware

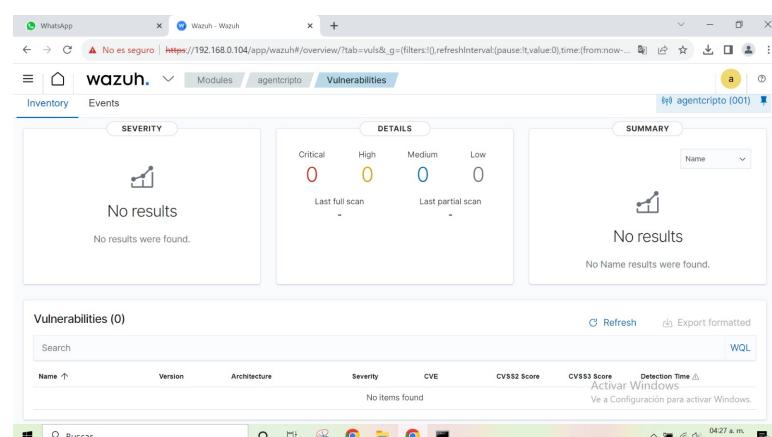


Figura 15: Vulnerabilidades antes de la ejecución del malware

The screenshot shows the Wazuh Security configuration assessment interface. At the top, it displays the CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 results: Passed 114, Failed 276, Not applicable 4, Score 29%, and End scan Apr 16, 2024 @ 02:48:59.000. Below this, the 'Checks (394)' section lists 15500, 15501, 15502, 15503, 15505, 15506, 15507, 15508, 15509, and 15510. All checks are marked as Failed. A note at the bottom right says 'Activar Windows' with a link 'Ve a Configuración para activar Windows...'. The interface includes a search bar, refresh button, and export formatted button.

Figura 16: Security configuration assessment DESPUÉS de la ejecución del malware

This screenshot is identical to Figure 16, showing the same CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 results and the list of failed security checks (15500-15510). The 'Activar Windows' note is also present. The interface layout is consistent with Figure 16.

Figura 17: Security configuration assessment DESPUÉS de la ejecución del malware

The screenshot shows the Wazuh Inventory interface. At the top, it displays system details: Cores: 1, Memory: 2047.55 MB, Arch: x86\_64, Operating system: Microsoft Windows 10 Home 10.0.19045.2965, CPU: Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz, Host name: DESKTOP-55N5B4Q, Board serial: 0, and Last scan: Apr 16, 2024 @ 19:08:10.000. Below this, the 'Network interfaces (2)' section lists Ethernet and Loopback Pseudo-Interface 1 with their respective MAC addresses, states, MTUs, and types. The 'Network ports (31)' section lists various local ports, IP addresses, processes, states, and protocols. A note at the bottom right says 'Activar Windows' with a link 'Ve a Configuración para activar Windows...'. The interface includes a search bar, refresh button, and export formatted button.

Figura 18: Wazuh Inventory DESPUÉS de la ejecución del ransomware

The screenshot shows the Wazuh Security events interface. The title bar indicates 'WhatsApp' and 'Wazuh - Wazuh'. The main content area displays a table of security alerts. The columns are: Time, Technique(s), Tactic(s), Description, Level, and Rule ID. There are 10 entries in the table. The first entry is a scheduled service. The second and fourth entries are T1078 alerts for Windows logon success. The fifth entry is another scheduled service. The sixth and eighth entries are T1078 alerts for Windows logon success. The seventh entry is a scheduled service. The ninth entry is a T1078 alert for Windows logon success with a note to activate Windows. The tenth entry is another T1078 alert for Windows logon success with a note to activate Windows. The bottom status bar shows the date as '16/04/2024' and the time as '07:19 p.m.'.

Figura 19: Wazuh Security alerts DESPUÉS de la ejecución del ransomware

The screenshot shows the Wazuh Security events interface. The title bar indicates 'WhatsApp' and 'Wazuh - Wazuh'. The main content area displays a table of security alerts. The columns are: Time, Technique(s), Tactic(s), Description, Level, and Rule ID. There are 10 entries in the table. The first entry is an SCA summary for CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0. The second entry is a CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 alert for ensuring network access. The third entry is a CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 alert for maximum password age. The fourth entry is a system time changed alert. The fifth entry is another system time changed alert. The sixth entry is a scheduled service. The seventh entry is a T1078 alert for Windows logon success with a note to activate Windows. The eighth entry is another T1078 alert for Windows logon success with a note to activate Windows. The bottom status bar shows the date as '16/04/2024' and the time as '07:20 p.m.'.

Figura 20: Wazuh Security alerts DESPUÉS de la ejecución del ransomware

En el caso del agente para Debian 12, el proceso de instalación del agente es prácticamente el mismo salvo por la elección de la arquitectura y el paquete, que en nuestro caso será DEB amd64. Desde la interfaz del dashboard, nos dirigimos a la sección de *add agent* y llenamos los campos pertinentes, al final, tendremos el siguiente link para instalar el agente dentro de Debian y después de ello reiniciar los servicios correspondientes:

**Run the following commands to download and install the agent:**

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.1.71' WAZUH_AGENT_NAME='Debian12' dpkg -i ./wazuh-
agent_4.7.3-1_amd64.deb
```

**Requirements**

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

**Start the agent:**

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Figura 21: Link y comandos para el agente Debian

Una vez que ejecutamos con éxito los comandos anteriores dentro de la máquina virtual con Debian 12, podremos ver al agente registrado dentro de la interfaz de Wazuh:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Debian12	10.0.2.15	default	Debian GNU/Linux 12	node01	v4.7.3	● active ⓘ	⟳ 🔍

Figura 22: Agente Debian ya registrado

Para activar el modulo de detección de vulnerabilidades en ambos casos, debemos de modificar el archivo de configuración presente en la ruta /var/ossec/etc/ossec.conf para Debian, en Windows podemos modificar dicho archivo desde la interfaz de Wazuh yendo a management → configuration → edit configuration, ahí debemos de cambiar dentro de la sección *vulnerability-detector* la sección de *enabled* cambiando el no por yes, lo mismo para las vulnerabilidades de los sistemas operativos que deseemos monitorear y finalmente reiniciar el manager.

```

GNU nano 7.2          /var/ossec/etc/ossec.conf
<enabled>yes</enabled>
<scan_on_start>yes</scan_on_start>
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>

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

<!-- Ubuntu OS vulnerabilities -->
<provider name="canonical">
<enabled>no</enabled>
<os>trusty</os>
<os>xenial</os>
<os>bionic</os>
<os>focal</os>
<os>jammy</os>

```

Figura 23: Activación del modúlo de vulnerabilidades

Ya que se logra esto, podremos ver activada la sección si nos vamos a management → configuration → vulnerabilities:

Vulnerabilities **ENABLED**  
Discover what applications are affected by well-known vulnerabilities

General Providers

Main settings  
General settings applied to the vulnerability detector and its providers

Vulnerability detector status	enabled
Interval between scan executions	300
Scan on start	yes

Figura 24: Modulo de vulnerabilidades ya activo

Es entonces que tenemos las siguientes vistas antes y después de nuestros ataques en Debian:

wazuh.

Inventory Dashboard Events

DebianPrueba (001)

manager.name: immerwahr rule.groups: syscheck agent.id: 001 + Add filter

There are no results for selected time range. Try another one.

Figura 25: Integrity monitoring antes de modificar el directorio /etc/

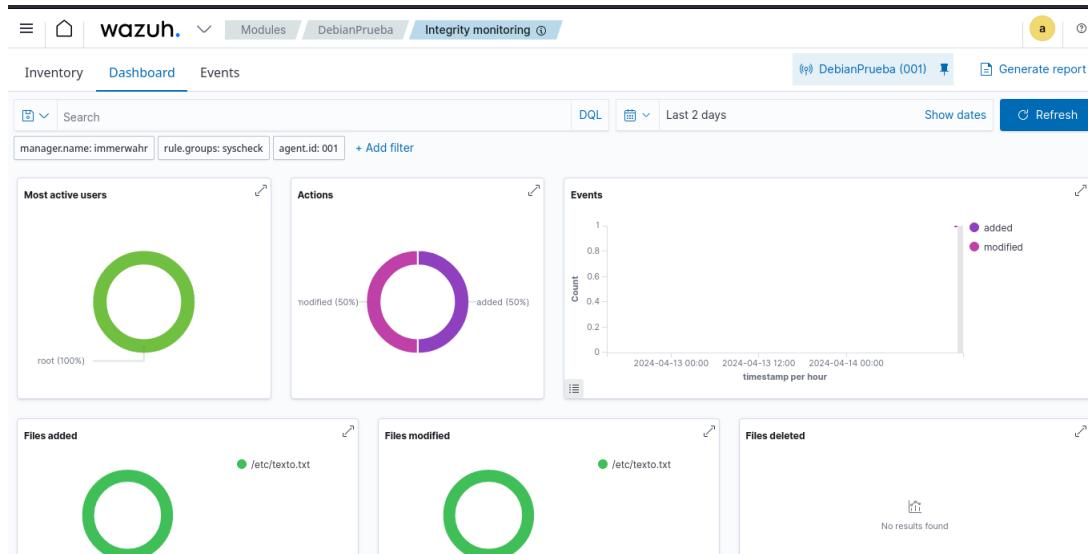


Figura 26: Integrity monitoring después de modificar el directorio /etc/ (para probar que funciona)

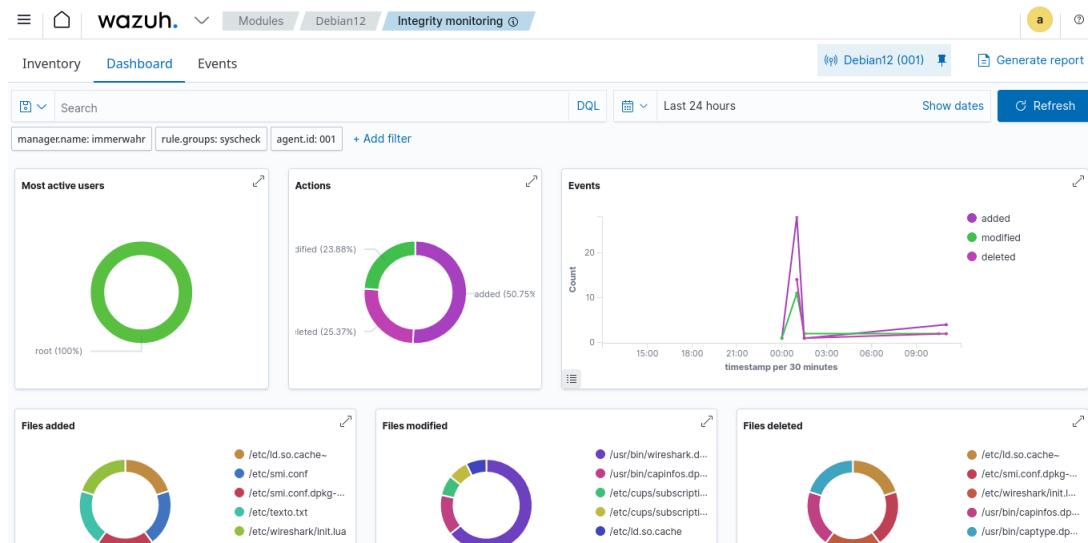


Figura 27: Integrity monitoring después de usar nuestro spyware

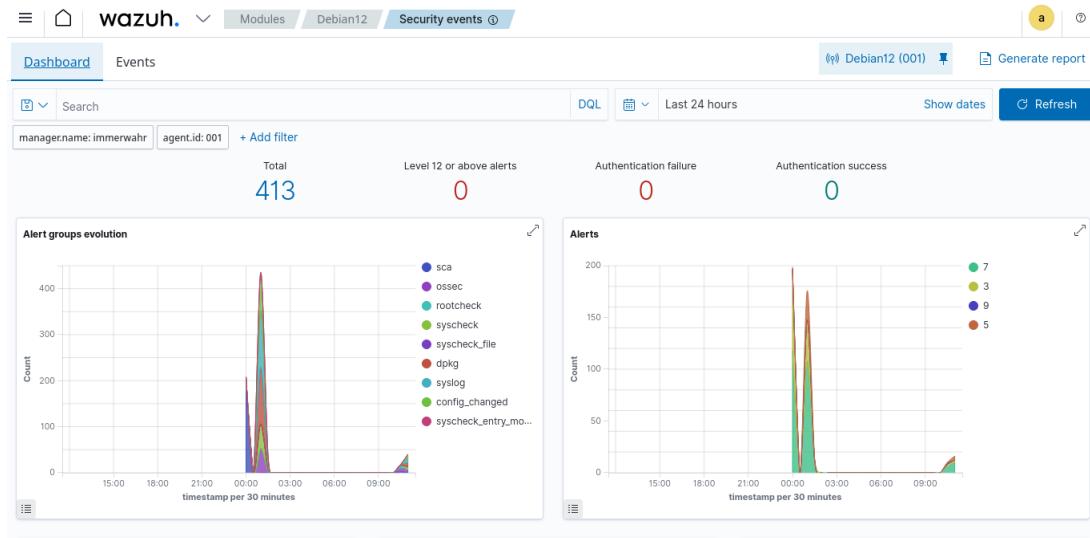


Figura 28: Security events antes y después del ataque por diccionario (no lo detectó)

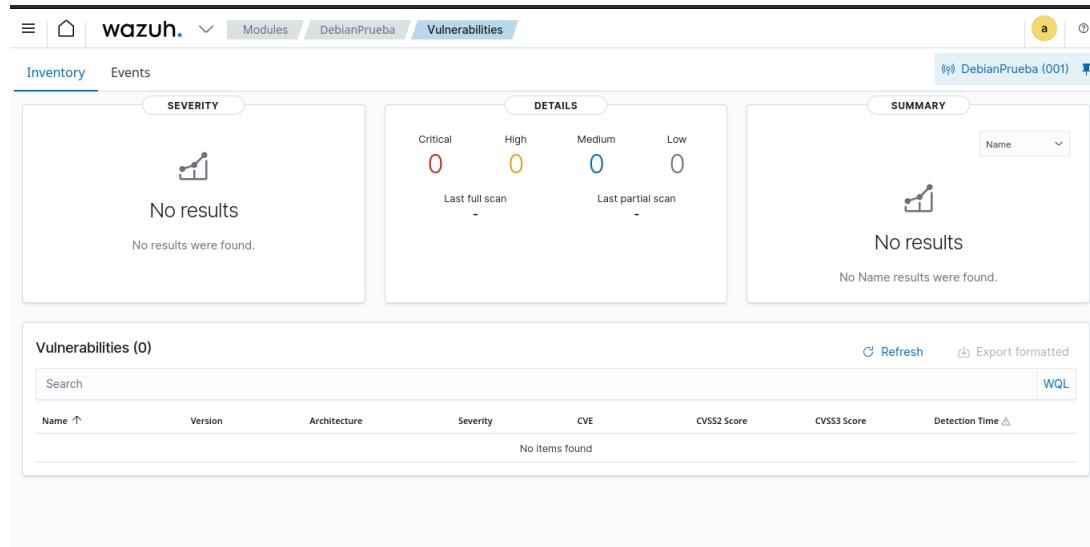


Figura 29: Vulnerabilities antes y después de los ataques (no reportó nada)

Además de lo anterior, en Debian tuvimos que habilitar el tráfico a través de los puertos 1514, 1515 y 55000 mediante el comando

```
1 firewall-cmd --permanent --add-port=numero/tcp
```

También requerimos de instalar openssh en la mv con el agente y en la máquina con el manager, además de hydra y nmap tal y como se vio en la práctica 5.

---

Del agente **agentcript** instalado en la MV con windows 10 tenemos los siguientes 5 test que no pasó

1. Ensure Audit Authentication Policy Change is set include Success: Esta alerta informa acerca de los cambios en la política de autenticación. Por decir algunos eventos de esta subcategoría son; se creo una nueva confianza para un dominio, Se modificó una entrada de información de bosque confiable, Se detectó una colisión de espacio de nombres, se agregó una entrada de información forestal confiable, etc.
2. Ensure Audit IPsec Driver: Los eventos de esta subcategoría incluyen: - 4960: IPsec descartó un paquete entrante que no pasó una verificación de integridad. Si este problema persiste, podría indicar un problema de red o que los paquetes se están modificando en tránsito a esta computadora. Verifique que los paquetes enviados desde la computadora remota sean los mismos que los recibidos por esta computadora. Este error también podría indicar problemas de interoperabilidad con otras implementaciones de IPsec. - 4961: IPsec descartó un paquete entrante que no pasó la verificación de reproducción. Si este problema persiste, podría indicar un ataque de repetición contra esta computadora. Si la alerta persiste podemos verificar si realmente los paquetes enviados desde la computadora remota son los mismo que los recibidos por esta computadora.
3. Ensure Interactive Logon: Smart card remove behavior. A veces, los usuarios olvidan bloquear sus estaciones de trabajo cuando están lejos de ellas, lo que permite que usuarios malintencionados accedan a sus computadoras. Forzar cierre de sesión o Desconexión si se trata de una sesión de Servicios de Escritorio remoto.
4. Ensure Microsoft network client: El secuestro de sesión utiliza herramientas que permiten a los atacantes que tienen acceso a la misma red que el cliente o servidor interrumpir, finalizar o robar una sesión en curso. Los atacantes pueden potencialmente interceptar y modificar paquetes SMB no firmados y luego modificar el tráfico y reenviarlo para que el servidor pueda realizar acciones no deseadas. Solución, firmar digitalmente las comunicaciones (siempre).
5. User Account Control: Esta configuración informa al usuario de que un programa requiere el uso de operaciones con privilegios elevados y requiere que el usuario pueda proporcionar credenciales administrativas para que el programa se ejecute. Se busca mitigar que los programas maliciosos se ejecuten con credenciales elevadas sin que el usuario o administrador sea consciente de su actividad. solución, denegar automáticamente solicitudes de elevación.

Del agente instalado en la MV con Debian 12 tenemos los siguientes 5 test que no pasó

1. Verificación de contraseñas encriptadas: Esta prueba asegura que todas las cuentas de usuario en el archivo /etc/passwd estén utilizando contraseñas encriptadas almacenadas en el archivo /etc/shadow, lo que mejora la seguridad de las contraseñas. Se soluciona haciendo uso de la herramienta passwd para asignar contraseñas encriptadas a los usuarios que haga falta o usar el comando sed -e 's/([a-zA-Z0-9.]\*):[^\*:]/1:x:/ -i /etc/passwd.
2. Verificación sobre los permisos de /etc/gshadow: Esta prueba asegura que solo los usuarios autorizados tengan acceso de lectura y escritura a este archivo (donde se almacena información importante sobre las contraseñas), para evitar posibles abusos o ataques. Se soluciona ajustando los permisos de dicho archivo mediante el comando chmod para asegurar que sólo el propietario tenga los permisos necesarios.
3. Auditoría de logs: Consiste en verificar y asegurar que los registros del sistema estén configurados adecuadamente para capturar eventos importantes y críticos que puedan indicar actividades sospechosas o maliciosas en el sistema. Se puede solucionar revisando la configuración de los registros del sistema y asegurándose de que esté correctamente establecida para capturar los eventos importantes y críticos. Para ello revisamos los archivos de configuración del registro como syslog-ng, rsyslog o systemd-journal y nos aseguramos de que estén correctamente configurados.
4. Auditoría de archivos de configuración de red: Esta prueba que la configuración de archivos de red críticos, como /etc/hosts.allow y /etc/hosts.deny, solo permita el acceso desde hosts y servicios autorizados. Por ejemplo, configuraciones incorrectas en estos archivos podrían permitir accesos no deseados a servicios de red. Se soluciona modificando los permisos presentes en dichos archivos, se revisa si hay reglas demasiado permisivas en /etc/hosts.allow o reglas contradictorias entre /etc/hosts.allow y /etc/hosts.deny y se ajustan según sea necesario.

- 
5. Verificación sobre los redireccionamientos ICMP: Los ICMP redirects son mensajes utilizados por los routers para indicar a un host que utilice una ruta diferente para enviar paquetes a un destino específico. Si estos mensajes no están controlados adecuadamente, podrían ser utilizados por atacantes para redirigir tráfico a través de rutas no autorizadas, lo que podría resultar en que nuestro tráfico sea interceptado o en ataques de denegación de servicio. Se puede arreglar este inconveniente configurando el kernel para que no acepte ICMP redirects. Se puede configurar el parametro net.ipv4.conf.all.accept\_redirects en el archivo /etc/sysctl.conf y establecer su valor en 0.

---

### 3. Conclusión

Hemos observado a lo largo de la elaboración de esta práctica sobre los numerosos beneficios que ofrece la herramienta de seguridad cibernética wazuh (de código abierto y libre) ya que nos ayuda a detectar una gran cantidad amenazas o intrusos contra cualquier equipo(s) que deseemos monitorear y/o aumentar su seguridad con la instalación de agentes. Funciona mediante la recolección de eventos de seguridad, lleva un registro acerca de las vulnerabilidades en el sistema, incluso provee demás opciones de seguridad como firewalls y SIEMS. Como ya hemos visto con anterioridad, funciona para varios sistemas operativos como windows, linux y se sabe que también esta diseñado para funcionar con AIX, HP-UX, macOS y Solaris. El servidor de wazuh nos permite además de recibir y recopilar datos, enviar ordenes a los agentes para responder cuando se detecta alguna amenaza en el equipo. Lo anterior, nos ayuda a mitigar problemas como lo son *ransomwares* o *spywares* al detectarlos de una manera mucho más temprana y sencilla a comparación si se realiza manualmente. En conclusión wazuh es una herramienta que nos brinda seguridad informática al detectar y dar respuesta a amenazas o peligros en nuestros equipos en tiempo real, siendo de mucha mayor utilidad en lugares como lo son empresas grandes e importantes que suelen tener una gran cantidad de equipos y altas probabilidades de ser atacados por usuarios maliciosos.

### 4. Referencias

- Wazuh. Recuperado el 12 de Abril de 2024 <https://wazuh.com/>
- Wazuh. (s/f). Installing Wazuh agents on Windows endpoints. Wazuh.com. Recuperado el 17 de abril de 2024, de <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>
- Wikipedia contributors. (s/f). Wazuh. Wikipedia, The Free Encyclopedia. <https://es.wikipedia.org/w/index.php?title=Wazuh&oldid=158175602>
- Tech, E. (2023, abril 10). ¿Qué es Wazuh y cómo funciona en la protección de sistemas? Medium. <https://medium.com/@ehztech/wazuh-75731fcff4ab>