

Integración complementaria de reglas YARA

Para realizar la integración del agente de Wazuh con Yara en los host terminales monitorizados se utilizarán las reglas de Wazuh manager de la prueba de concepto junto con un repositorio de Github de yara para realizar la integración complementaria.

Para la instalación de un agente de Wazuh integrado con Yara se propone un script que automatiza el proceso de instalación e integración de estas 2 herramientas en un terminal Linux.

```
#!/bin/bash
# 1. Revisión de la actualización de repositorios
# 2. El proceso se mostrara paso a paso para identificacion de posibles fallas
set -x
sudo apt install curl
sudo apt install git

# 2. Instalacion de claves GPG Wazuh
sudo curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring
gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
sleep 3

# 3. Añadiendo el repositorio de Wazuh
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable
main" | tee -a /etc/apt/sources.list.d/wazuh.list
read -p 'Introduzca el nombre del agente (minúsculas en formato nombre.apellido): ' nombre

# 4. Descarga e inicialización del agente wazuh.deb
curl -so wazuh-agent_4.7.3-1_amd64.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-
agent/wazuh-agent_4.7.3-1_amd64.deb && sudo WAZUH_MANAGER="172.28.1.69" WAZUH_AGENT_GROUP="UGTD"
WAZUH_AGENT_NAME="$nombre" dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb
```

```
sleep 3
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
sleep 3

# El proceso se mostrara paso a paso para identificacion de posibles fallas
set -x

# 5. Descarga YARA y sus dependencias
sudo apt install -y make gcc autoconf libtool libssl-dev pkg-config jq
sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz
sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/ && rm -f v4.2.3.tar.gz
cd /usr/local/bin/yara-4.2.3/
sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make install && sudo make check
sleep 5
sudo echo "/usr/local/lib" >> /etc/ld.so.conf
sleep 3
ldconfig

# 6. Preparación de reglas Yara
sudo apt-get update
sudo mkdir -p /var/ossec/yara/rules
sudo chmod 771 /var/ossec/yara/rules

# 7. Clonar el repositorio de Git en /var/ossec/yara
git clone https://github.com/Yara-Rules/rules.git /var/ossec/yara/rules
sleep 1

# Archivo de reglas YARA de Valhalla
sudo curl 'https://valhalla.nexttron-systems.com/api/v1/get' \
-H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8' \
-H 'Accept-Language: en-US,en;q=0.5' \
--compressed \
-H 'Referer: https://valhalla.nexttron-systems.com/' \
-H 'Content-Type: application/x-www-form-urlencoded' \
-H 'DNT: 1' -H 'Connection: keep-alive' -H 'Upgrade-Insecure-Requests: 1' \
--data
```

[illegible]

El script de generación de índices para Yara complementa las reglas descritas en el repositorio de Github con las reglas Yara utilizadas para la prueba de concepto y se incluye en la descarga del repositorio en el paso 7 del script de instalación.

```
/*
Generated by Yara-Rules
On 19-04-2024
```

```
*/  
include "./antidebug_antivm/antidebug_antivm.yar"  
include "./capabilities/capabilities.yar"  
include "./crypto/crypto_signatures.yar"  
include "./cve_rules/CVE-2010-0805.yar"  
include "./cve_rules/CVE-2010-0887.yar"  
  
.  
.  
.  
  
include "./yara_rules.yar"
```

Pasada la primera etapa se configura el archivo ossec.conf del agente en `/var/ossec/etc/ossec.conf` dentro del modulo de syscheck.

```
<syscheck>  
  
...  
<directories realtime=\"yes\">Directorio_Monitorizado</directories>  
...  
  
</syscheck>
```

Reinicio del agente

```
sudo systemctl restart wazuh-agent
```

Comprobación del estado del agente

```
sudo systemctl status wazuh-agent
```

Se sugiere la modificación del script de yara para que se dirija al nuevo archivo de reglas que resulta ser index.yar.

```
#!/bin/bash  
# Wazuh - Yara active response  
# Copyright (C) 2015-2022, Wazuh Inc.  
# This program is free software; you can redistribute it  
# and/or modify it under the terms of the GNU General Public
```

```

# License (version 2) as published by the FSF - Free Software
# Foundation.

#----- Gather parameters -----#

# Extra arguments
read INPUT_JSON
#YARA_PATH=$(echo $INPUT_JSON | jq -r .parameters.extra_args[1])
#YARA_RULES=$(echo $INPUT_JSON | jq -r .parameters.extra_args[3])
YARA_PATH="/usr/local/bin/yara-4.2.3"
YARA_RULES="/var/ossec/yara/rules/index.yar"
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.syscheck.path)

# Set LOG_FILE path
LOG_FILE="logs/active-responses.log"
size=0
actual_size=$(stat -c %s ${FILENAME})
while [ ${size} -ne ${actual_size} ]; do
    sleep 1
    size=${actual_size}
    actual_size=$(stat -c %s ${FILENAME})
done
#----- Analyze parameters -----#
if [[ ! $YARA_PATH ]] || [[ ! $YARA_RULES ]]
then
    echo "wazuh-yara: ERROR - Yara active response error. Yara path and rules parameters are
mandatory." >> ${LOG_FILE}
    exit 1
fi
#----- Main workflow -----#
# Execute Yara scan on the specified filename
yara_output="$( "${YARA_PATH}" /yara -w -r "$YARA_RULES" "$FILENAME" )"
if [[ $yara_output != "" ]]
then
    # Iterate every detected rule and append it to the LOG_FILE
    while read -r line; do
        echo "wazuh-yara: INFO - Scan result: $line" >> ${LOG_FILE}
    done <<< "$yara_output"
fi

```

```
exit 0;
```

En el script se modificaron los parámetros de YARA_PATH y YARA_RULES de acuerdo a la version de yara en path, y al nuevo archivo de reglas en YARA_RULES.

Revision #2

Created 6 mayo 2024 16:16:38 by Ricardo Alberto

Updated 7 mayo 2024 11:30:52 by Ricardo Alberto