

- *Đối với máy Agent Ubuntu*

Bước 1: Cấu hình Wazuh Agent: cấu hình tệp ossec.conf: theo dõi nhật ký truy cập Apache

nano /var/ossec/etc/ossec.conf

Ctrl+W để search: gõ <localfile> , xong nhấn Enter và thêm đoạn script sau:

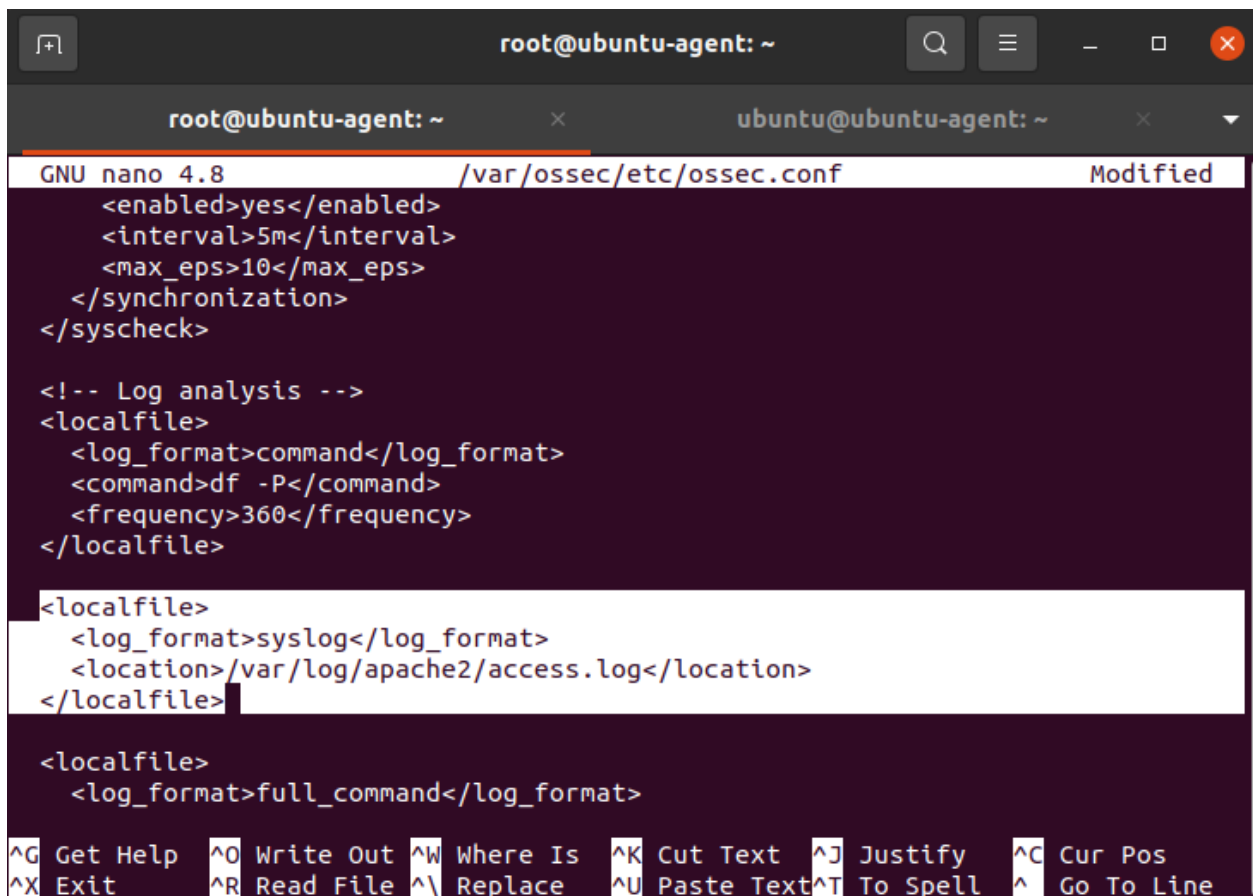
```
<localfile>

<log_format>syslog</log_format>

<location>/var/log/apache2/access.log</location>

</localfile>
```

Ctrl+X nhấn y, Enter để lưu



```
root@ubuntu-agent: ~
GNU nano 4.8 /var/ossec/etc/ossec.conf Modified
<enabled>yes</enabled>
<interval>5m</interval>
<max_eps>10</max_eps>
</synchronization>
</syscheck>

<!-- Log analysis -->
<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>

<localfile>
  <log_format>full_command</log_format>

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace  ^U Paste Text ^T To Spell  ^ Go To Line
```

Hình 24. Cấu hình tệp ossec.conf

Script này là khối lệnh theo dõi nhật ký truy cập Apache

Bước 5: Khởi động lại Wazuh Agent để áp dụng các thay đổi

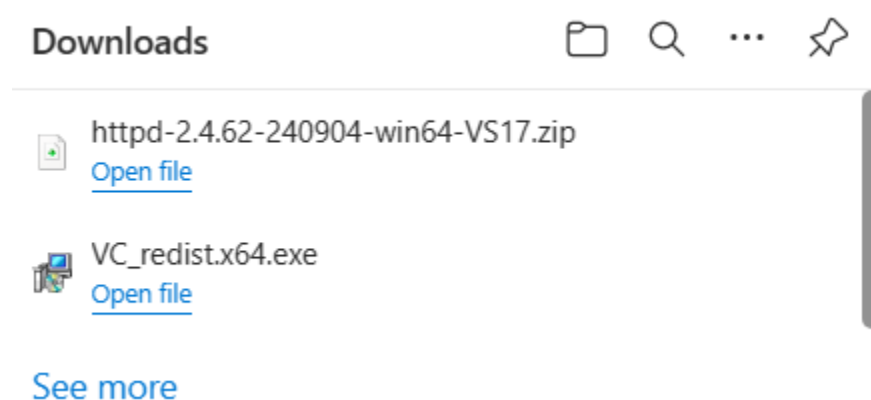
`systemctl restart wazuh-agent.service`

- **Đối với máy Agent Windows Server**

Bước 1: Cài đặt Web Apache

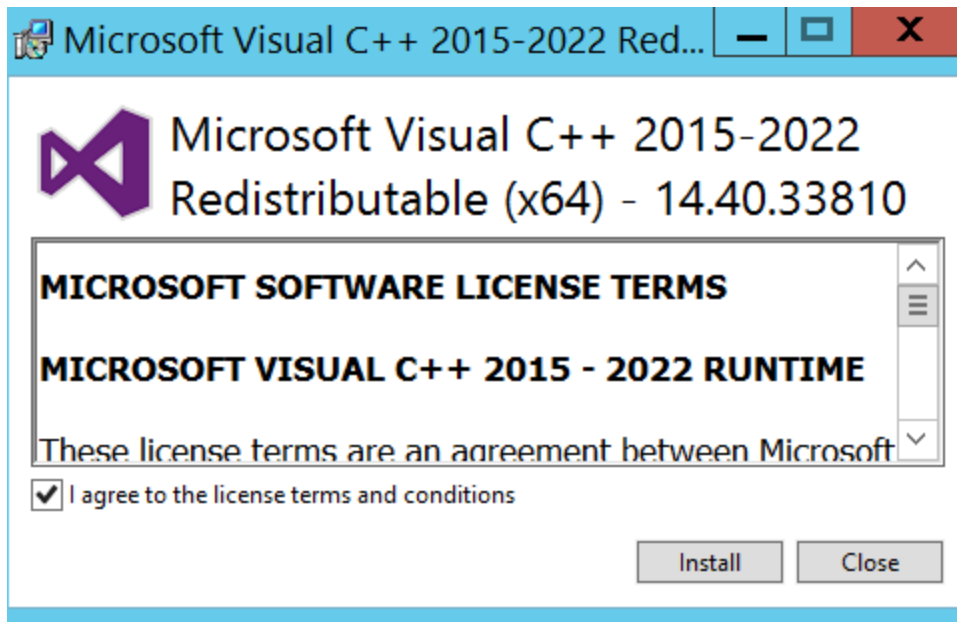
Cài Visual C++ Redistributable Visual Studio và file apache theo link sau:

<https://www.apachelounge.com/download/>



Hình 25. Download apache và visual code redist cho Windows Server 2012

Cài đặt vc_redist trước

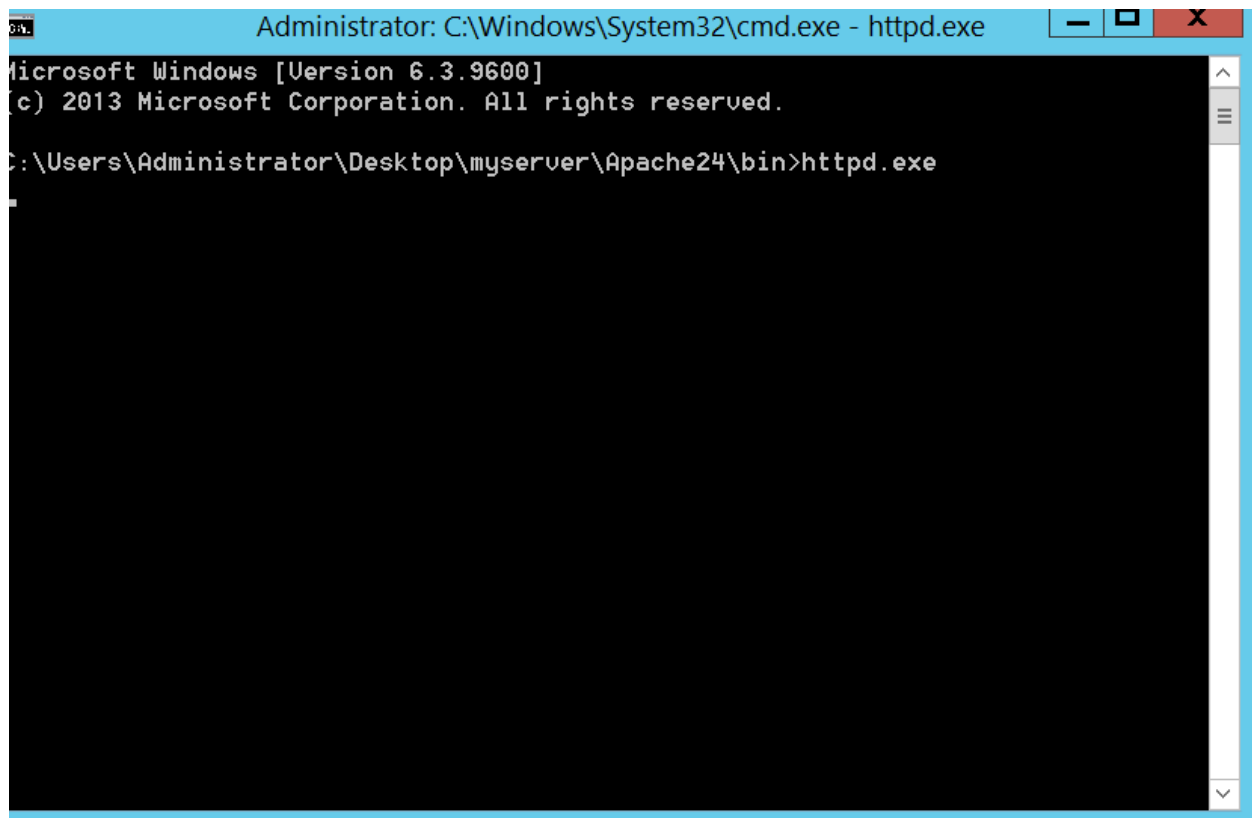


Hình 26. Cài đặt vc_redist

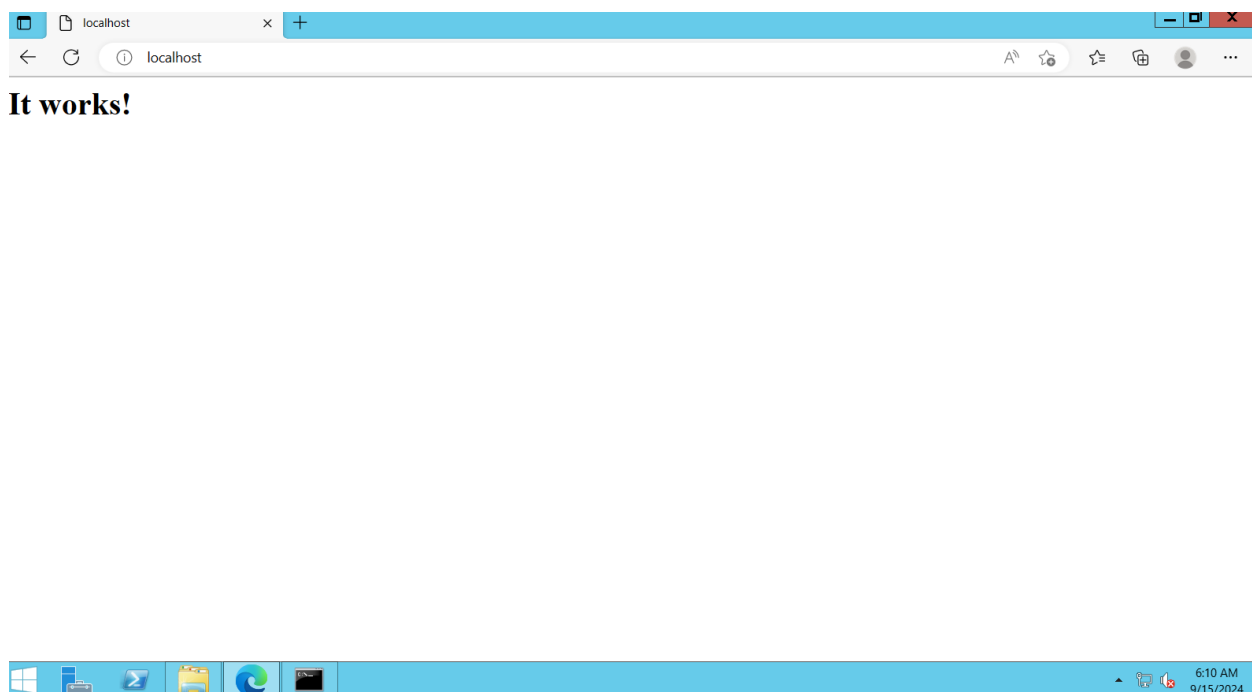
Tiếp theo cài đặt apache theo link hướng dẫn sau:

<https://www.bing.com/videos/riverview/relatedvideo?q=web+apache+download+for+windows+server+2012&mid=929BC09D85BB9ECB2E7C929BC09D85BB9ECB2E7C&FORM=VIRE>

Bước 2: Chạy và kiểm tra trạng thái Apache



Hình 27. Chạy httpd.exe



Hình 28. Web apache đang hoạt động trên Windows Server 2012

Bước 3: Cấu hình Wazuh Agent



```
<!-- Agent buffer options -->
<client_buffer>
  <disabled>no</disabled>
  <queue_size>5000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

<!-- Log analysis -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>C:\Users\Administrator\Desktop\myserver\Apache24\logs\access.log</location>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
```

Script này là khối lệnh theo dõi nhật ký truy cập Apache

Bước 4: Khởi động lại Wazuh agent để áp dụng các thay đổi

Mở PowerShell

Restart-Service -Name WazuhSvc

Hoặc

Restart-Service -Name wazuh

- *Đối với máy Wazuh Server*

Bước 1: Cài đặt tiện ích wget

apt update && apt install -y wget

Bước 2: Tải cơ sở dữ liệu của alienvault ip

```
wget https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/alienvault_reputation.ipset -O /var/ossec/etc/lists/alienvault_reputation.ipset
```

Bước 3: Thêm địa chỉ ip attacker vào cơ sở dữ liệu alienvault ip

```
echo "192.168.198.129" >> /var/ossec/etc/lists/alienvault_reputation.ipset
```

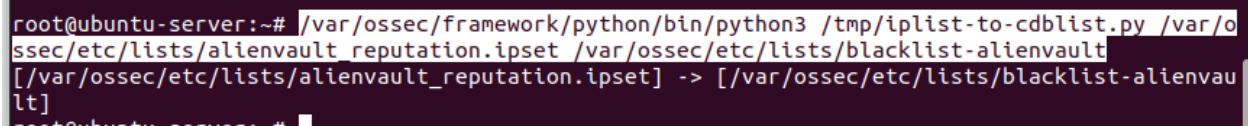
192.168.198.129 là địa chỉ của attacker

Bước 4: Tải script để chuyển đổi định dạng tệp

```
wget https://wazuh.com/resources/iplist-to-cdblist.py -O /tmp/iplist-to-cdblist.py
```

Bước 5: Chuyển đổi định dạng alienvault .ipset sang định dạng .gpg

```
/var/ossec/framework/python/bin/python3 /tmp/iplist-to-cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/lists/blacklist-alienvault
```



```
root@ubuntu-server:~# /var/ossec/framework/python/bin/python3 /tmp/iplist-to-cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/lists/blacklist-alienvault
[/var/ossec/etc/lists/alienvault_reputation.ipset] -> [/var/ossec/etc/lists/blacklist-alienvault]
```

Bước 6: Xóa tệp không cần thiết

```
rm -rf /var/ossec/etc/lists/alienvault_reputation.ipset
```

```
rm -rf /tmp/iplist-to-cdblist.py
```

Bước 7: Gán quyền cho tệp /var/ossec/etc/lists/blacklist-alienvault

```
chown wazuh:wazuh /var/ossec/etc/lists/blacklist-alienvault
```

Bước 8: Kích hoạt tập lệnh active response

```
nano /var/ossec/etc/rules/local_rules.xml
```

```

<group name="attack">

  <rule id="100100" level="10">

    <if_group>web|attack|attacks</if_group>

    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-
alienvault</list>

    <description>IP address found in AlientVault reputation database</description>

  </rule>

</group>

```

```

GNU nano 6.2 /var/ossec/etc/rules/local_rules.xml *
<!--
Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
-->
<rule id="100001" level="5">
  <if_sid>5716</if_sid>
  <srcip>1.1.1.1</srcip>
  <description>sshd: authentication failed from IP 1.1.1.1.</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>

</group>

<group name="attack">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in AlientVault reputation database</description>
  </rule>
</group>

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line

```

Bước 9: Cấu hình Wazuh Server

Thêm quy tắc để kích hoạt tập lệnh phản hồi vào tập bộ quy tắc local rules

nano /var/ossec/etc/ossec.conf

Thêm:

```
<list>etc/lists/blacklist-alienvault</list>
```

```
<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <rule_exclude>0215-policy_rules.xml</rule_exclude>
  <list>etc/lists/audit-keys</list>
  <list>etc/lists/amazon/aws-eventnames</list>
  <list>etc/lists/security-eventchannel</list>
  <list>etc/lists/blacklist-alienvault</list>

  <!-- User-defined ruleset -->
  <decoder_dir>etc/decoders</decoder_dir>
  <rule_dir>etc/rules</rule_dir>

```

G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^ Go To Line

#For Ubuntu endpoint

```
<ossec_config>
```

```
<active-response>
```

```
<command>firewall-drop</command>
```

```
<location>local</location>
```

```
<rules_id>100100</rules_id>
```

```
<timeout>120</timeout>
```

```
</active-response>
```

```
</ossec_config>
```

#Script này ngăn kết nối mạng đến từ điểm cuối của attacker Ubuntu trong 120s

#For Windows endpoint

```
<ossec_config>
```

```
<active-response>
```

```
<command>netsh</command>
```



```
<location>local</location>
```

```
<rules_id>100100</rules_id>
```

```
<timeout>120</timeout>
```

```
</active-response>
```

```
</ossec_config>
```

#Script này sẽ chặn IP attacker Windows trong 120s

```
GNU nano 6.2 /var/ossec/etc/ossec.conf
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/dpkg.log</location>
</localfile>

</ossec_config>

#For Ubuntu endpoint
<ossec_config>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>120</timeout>
  </active-response>
</ossec_config>

#For Windows endpoint
<ossec_config>
  <active-response>
    <command>netsh</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>120</timeout>
  </active-response>
</ossec_config>
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line

Bước 10: Khởi động lại Wazuh Server để áp dụng các thay đổi

```
systemctl restart wazuh-manager.service
```

- **Trên máy attacker truy cập vào máy chủ web apache agent ubuntu**
Giả lập tấn công bằng lệnh sau:

curl http://192.168.198.148
192.168.198.148: địa chỉ ip web apache agent ubuntu

Kết quả: Vào wazuh server để xem cảnh báo:

- Phát hiện địa chỉ IP truy cập vào web server

Security Alerts					
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Sep 30, 2024 @ 22:20:09.772			IP address found in AlienVault reputation database	10	100100
Table JSON Rule					
@timestamp	2024-09-30T15:20:09.772Z				
_id	jm-EQ5lB093sm6xshpgT				
agent.id	001				
agent.ip	192.168.198.148				
agent.name	ubuntu-agent				
data.id	200				
data.protocol	GET				
data.srcip	192.168.198.129				
data.uri	/				
decoder.name	web-accesslog				
full_log	192.168.198.129 - - [30/Sep/2024:22:20:09 +0700] "GET / HTTP/1.1" 200 10926 "-" *curl/8.8.0"				
id	1727709609.4213246				
input.type	log				
location	/var/log/apache2/access.log				
manager.name	anh-atit				
rule.description	IP address found in AlienVault reputation database				

- Sau đó wazuh đã block địa chỉ IP đó trong 120s

Sep 30, 2024 @ 22:22:10.780	Host Unblocked by firewall-drop Active Response	3	652
Sep 30, 2024 @ 22:20:10.637	Host Blocked by firewall-drop Active Response	3	651

- Trên máy attacker truy cập vào máy chủ web apache agent windows server

Giả lập tấn công bằng lệnh sau:
curl http://192.168.198.149
192.168.198.149: địa chỉ ip web apache agent windows server

```
(root@kali)-[~]
# curl http://192.168.198.149
<html><body><h1>It works!</h1></body></html>
```

Kết quả: Vào wazuh server để xem cảnh báo:

- Phát hiện địa chỉ IP truy cập vào web server




✓	Sep 30, 2024 @ 23:02:45.796	IP address found in AlienVault reputation database	10	100100
---	-----------------------------	--	----	--------

Table	JSON	Rule
	@timestamp	2024-09-30T16:02:45.796Z
	_id	JhyrQ5IBMfnejZT3lrbr
	agent.id	002
	agent.ip	192.168.198.149
	agent.name	WIN-KM1IMIN1Q69
	data.id	200
	data.protocol	GET
	data.srcip	192.168.198.129
	data.url	/
	decoder.name	web-accesslog
	full_log	192.168.198.129 - - [30/Sep/2024:09:02:45 -0700] "GET / HTTP/1.1" 200 46

- Sau đó wazuh đã block địa chỉ IP đó trong 120s

✓	Sep 30, 2024 @ 23:02:47.273	Active response: active-response/bin/netsh.exe - add	3	657
---	-----------------------------	--	---	-----

able	JSON	Rule
	@timestamp	2024-09-30T16:02:47.273Z
	_id	JxyrQ5IBMfnejZT3jrBJ
	agent.id	002
	agent.ip	192.168.198.149
	agent.name	WIN-KM1IMIN1Q69
	data.command	add
	data.origin.module	wazuh-execd
	data.origin.name	node01
	data.parameters.alert.agent.id	002
	data.parameters.alert.agent.ip	192.168.198.149
	data.parameters.alert.agent.name	WIN-KM1IMIN1Q69
	data.parameters.alert.data.id	200

Table	JSON	Rule
	@timestamp	2024-09-30T16:04:48.323Z
	_id	OxyIQ5IBMfnejZT3d7bx
	agent.id	002
	agent.ip	192.168.198.149
	agent.name	WIN-KM11MIN1Q69
	data.command	delete
	data.origin.module	wazuh-execd
	data.origin.name	node01
	data.parameters.alert.agent.id	002
	data.parameters.alert.agent.ip	192.168.198.149
	data.parameters.alert.agent.name	WIN-KM11MIN1Q69
	data.parameters.alert.data.id	200
	data.parameters.alert.data.protocol	GET
  	data.parameters.alert.data.scrip	192.168.198.129