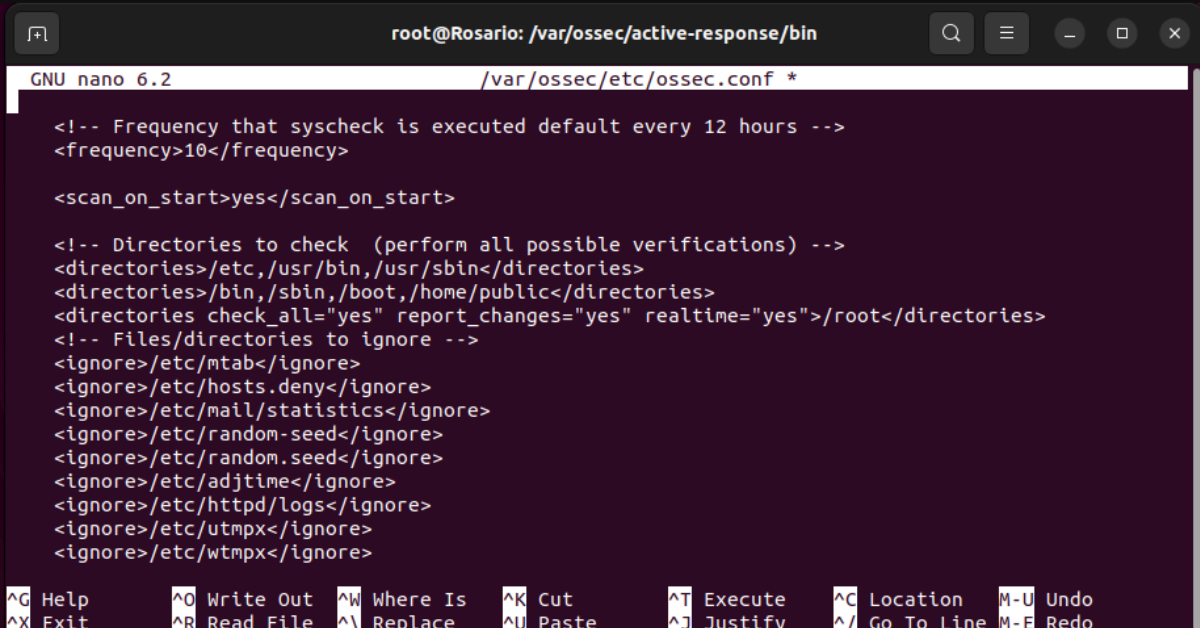


RILEVAZIONE DI FILE MALEVOLI TRAMITE VIRUSTOTAL E WAZUH

Questo lavoro presenta l'integrazione tra **Wazuh**, una piattaforma open-source per il monitoraggio della sicurezza, e **VirusTotal**, un servizio online che analizza file sospetti utilizzando oltre 70 antivirus e strumenti di rilevazione. La combinazione di queste tecnologie permette di costruire un sistema di rilevamento avanzato, capace di identificare file potenzialmente dannosi in modo tempestivo e accurato.

1) Aggiungiamo la funzione di "root check" nel file di configurazione dell'agent dell'endpoint:

```
<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>
```



```
root@Rosario: /var/ossec/active-response/bin
GNU nano 6.2 /var/ossec/etc/ossec.conf *
<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>10</frequency>

<scan_on_start>yes</scan_on_start>

<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot,/home/public</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>
<!-- Files/directories to ignore -->
<ignore>/etc/mtab</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/random.seed</ignore>
<ignore>/etc/adjtime</ignore>
<ignore>/etc/httpd/logs</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/wtmpx</ignore>

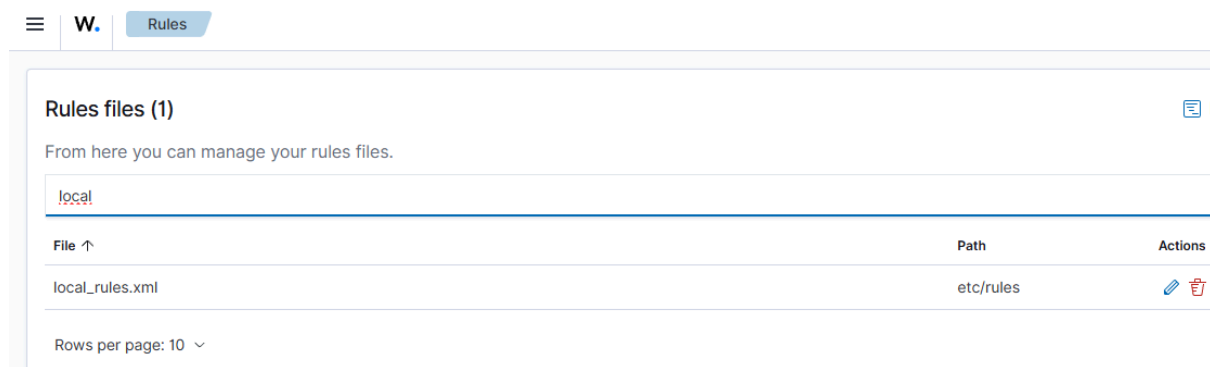
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line M-E Redo
```

Spiegazione dei parametri:

1. **<directories>**: Questo tag indica che Wazuh deve monitorare le directory specificate (in questo caso **/root**) per eventuali modifiche. Wazuh può monitorare il contenuto delle directory per rilevare cambiamenti, file nuovi o modifiche a file esistenti.
2. **check_all="yes"**: Impostato su **yes**, significa che Wazuh controllerà tutte le modifiche all'interno della directory **/root**, non limitandosi solo a file o tipi di cambiamento specifici. Ogni tipo di cambiamento (creazione, modifica, cancellazione di file) verrà tracciato.
3. **report_changes="yes"**: Impostato su **yes**, Wazuh genererà un report ogni volta che viene rilevata una modifica all'interno della directory monitorata. Questo è essenziale per tenere traccia delle attività sospette o non autorizzate, come la creazione di file in **/root** o modifiche a file critici.

4. **realtime="yes"**: Questo parametro fa sì che le modifiche vengano monitorate in tempo reale. Quando viene fatta una modifica, l'evento viene immediatamente registrato e inviato al server Wazuh per l'analisi. Ciò permette di rilevare attività in tempo reale, migliorando la reattività del sistema di monitoraggio.

2) A questo punto aggiungiamo la regola su **Wazuh** che tiene traccia dei cambiamenti nella root directory dell'endpoint, nelle local_rules infatti possiamo aggiungere delle regole custom:



Le regole :

```
<rule id="100200" level="7">  
  <if_sid>550</if_sid>  
  <field name="file">/root</field>  
  <description>File modified in /root directory</description>  
</rule>
```

```
<rule id="100201" level="7">  
  <if_sid>554</if_sid>  
  <field name="file">/root</field>  
  <description>File added to /root directory</description>  
</rule>
```

id="100200" e "100201": Identificatore univoco per la regola, utile per l'analisi dei log. Ogni regola ha un proprio ID.

level="7": Il livello di severità della regola. Un livello 7 indica un livello di attenzione abbastanza elevato, suggerendo che la modifica di un file nella directory **/root** potrebbe essere un'attività sospetta o pericolosa.

<if_sid>550</if_sid> <if_sid>554</if_sid>: Questo specifica che la regola si attiva se è presente un evento con l'ID 550, che potrebbe essere una regola che rileva una modifica su un file. In questo caso, stiamo cercando eventi correlati a modifiche ai file (ad esempio, modifiche di file di sistema o critici).

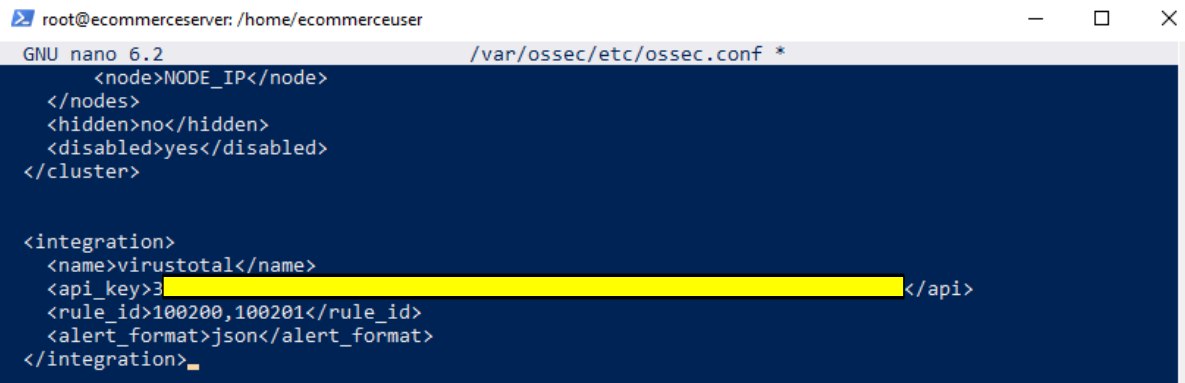
L'altra regola viene attivata quando un evento con l'ID 554 viene rilevato. Questo potrebbe corrispondere a un evento che segnala un'aggiunta di un file.

<field name="file">/root</field>: La regola è specifica per la directory **/root**. Wazuh monitorerà i file modificati all'interno di questa directory.

<description>File modified/added in /root directory</description>: Descrizione dell'azione che questa regola è destinata a rilevare: "Un file è stato modificato nella directory **/root**" o nell'altro caso che è stato aggiunto. Se un file nella directory **/root** viene modificato, l'evento verrà registrato e contrassegnato con il livello di severità 7.

Aggiornate le regole riavviamo il servizio del manager di **Wazuh**

3) Procediamo aggiungendo nel file di configurazione del manager di **Wazuh** il modulo integrazione per Virus Total:



```
root@ecommerceuser: /home/ecommerceuser
GNU nano 6.2 /var/ossec/etc/ossec.conf
<node>NODE_IP</node>
</nodes>
<hidden>no</hidden>
<disabled>yes</disabled>
</cluster>

<integration>
  <name>virustotal</name>
  <api_key>3[REDACTED]</api>
  <rule_id>100200,100201</rule_id>
  <alert_format>json</alert_format>
</integration>
```

Spiegazione della regola:

- **<integration>**: Questo tag definisce l'integrazione con un servizio esterno. In questo caso, il servizio esterno è **VirusTotal**, che verrà utilizzato per analizzare i file sospetti rilevati da Wazuh.
- **<name>virustotal</name>**: Indica il nome del servizio con cui Wazuh deve integrarsi. In questo caso, il servizio è **VirusTotal**, una piattaforma online per l'analisi di file e URL sospetti.
- **<api_key>**: La chiave API fornita da VirusTotal che consente a Wazuh di comunicare con il servizio e inviare richieste per l'analisi dei file. È importante mantenere questa chiave sicura, poiché fornisce accesso ai dati di VirusTotal.
- **<rule_id>100200,100201</rule_id>**: Specifica che l'integrazione con VirusTotal sarà attivata solo quando una delle seguenti regole viene attivata da Wazuh:
 - **Regola 100200**: File modificato nella directory **/root**.
 - **Regola 100201**: File aggiunto nella directory **/root**.
- Quando una di queste regole viene soddisfatta, Wazuh invierà i dettagli al servizio di VirusTotal per l'analisi.
- **<alert_format>json</alert_format>**: Indica che i dati relativi agli eventi di allarme che Wazuh invia a VirusTotal saranno nel formato JSON. Questo è il formato

utilizzato per trasmettere i dettagli degli allarmi in modo strutturato e leggibile dal servizio VirusTotal.

Funzionamento:

- Quando Wazuh rileva una modifica o un'aggiunta di file nella directory **/root** (in base alle regole 100200 o 100201), l'integrazione con **VirusTotal** viene attivata.
- Wazuh invierà i dettagli del file sospetto a **VirusTotal** per un'analisi approfondita.
- **VirusTotal** restituirà una risposta (nel formato JSON) che può essere utilizzata per determinare se il file è malevolo o sicuro.

4) Ora possiamo testare il sistema, scarichiamo nella root directory dell'endpoint un file malevolo, il file sarà "eicar.com".

L'EICAR (European Institute for Computer Antivirus Research) è una organizzazione che ha creato un **file di test** chiamato **eicar.com** per consentire agli utenti di testare i software antivirus senza utilizzare malware reali.

Il file **eicar.com** è un semplice file di testo che, quando viene eseguito, simula il comportamento di un virus, ma in realtà non è dannoso. È usato esclusivamente per verificare che il software antivirus stia funzionando correttamente e possa rilevare minacce.

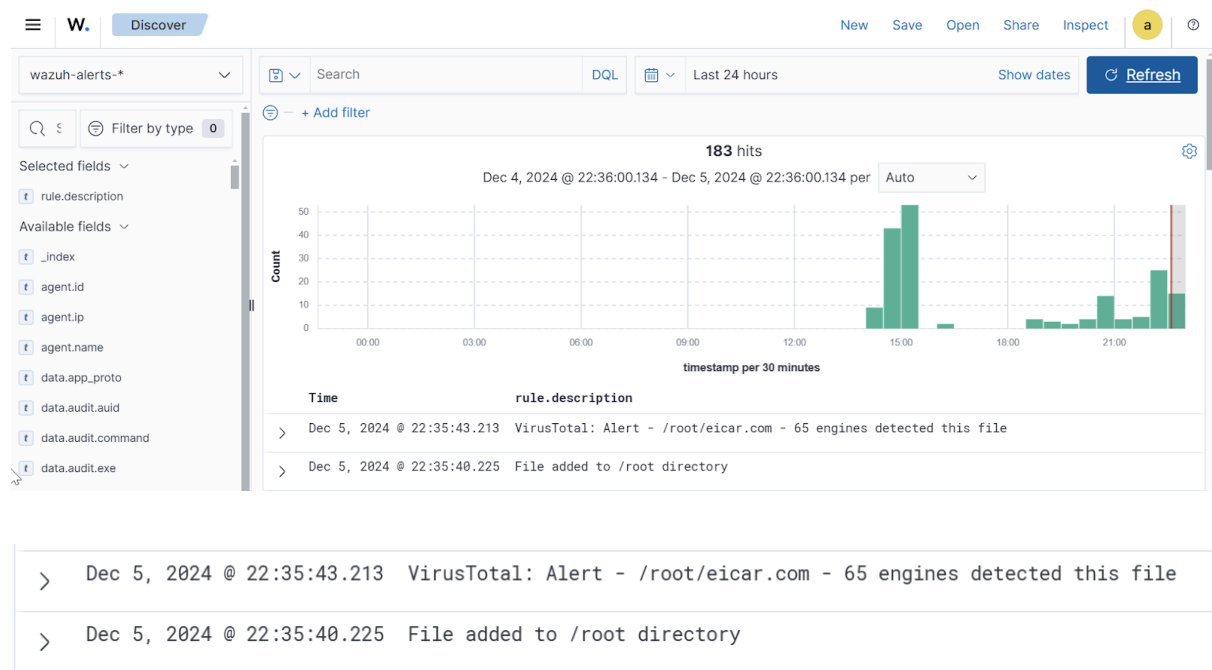
Quando si scarica il file **eicar.com** nella directory **/root** dell'endpoint, il sistema Wazuh, con le regole di monitoraggio configurate (come la regola per la modifica dei file in **/root**), dovrebbe rilevare l'aggiunta del file come evento sospetto. In particolare, il file aggiunto (nel nostro caso, **eicar.com**) attiverà la regola configurata (100201), che avvia l'integrazione con VirusTotal per una verifica più approfondita.

In sintesi, scaricare il **file eicar.com** è una simulazione sicura per testare la rilevazione di attività sospette nel sistema, senza rischiare danni reali.

```
root@Rosario:/var/ossec/active-response/bin# curl -Lo /root/eicar.com https://www.eicar.org/eicar.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left     Speed
  0     0     0      0     0      0      0      0  --:--:-- --:--:-- --:--:--     0
100 70386  100 70386     0     0    25498      0  --:--:--  0:00:02 --:--:-- 62233
```

```
root@Rosario:/var/ossec/active-response/bin# ls -lah /root/eicar.com
-rw-r--r-- 1 root root 69K Dez  5 21:50 /root/eicar.com
root@Rosario:/var/ossec/active-response/bin#
```

Verifichiamo sulla dashboard di **Wazuh** se il file viene rilevato e controllato su **VirusTotal** tramite l'integrazione implementata:



Come possiamo notare il file è stato rilevato come minaccia in base a 65 motori antivirus su **Virus Total**.