

RILEVARE E BLOCCARE ATTACCHI BRUTE FORCE SSH

Questa funzione di Wazuh permette di rilevare tentativi di accesso SSH non autorizzati e rispondere automaticamente bloccando l'IP dell'attaccante. Grazie alla configurazione delle regole e delle **Active Response**, il manager Wazuh identifica i tentativi di brute force e invia un comando all'agent per bloccare i pacchetti tramite firewall, proteggendo così il sistema in tempo reale.

Partiamo dalla configurazione del manager di **Wazuh**, configurando l'active response in questo modo:

```
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5763</rules_id>
  <timeout>180</timeout>
</active-response>
```

L'elemento configurato in `<active-response>` è una regola che esegue un'azione automatica (nel caso specifico, il comando `firewall-drop`) quando viene attivata la regola con ID **5763**.

<command>: Specifica il comando da eseguire quando la regola viene attivata. In questo caso, `firewall-drop` blocca l'IP responsabile dell'evento rilevato.

<location>: Indica dove deve essere eseguito il comando. `local` significa che verrà eseguito sulla macchina locale dove gira Wazuh Manager.

<rules_id>: ID della regola che attiva la risposta. Nel tuo esempio, la regola con ID **5763**.

<timeout>: Durata (in secondi) per cui il comando resta attivo. Ad esempio, un IP bloccato rimarrà tale per 180 secondi.

La regola a cui si fa riferimento la possiamo riscontrare nella dashboard di **Wazuh**:

< 0095-sshd_rules.xml

```
473 <rule id="5762" level="4">
474   <if_sid>5700</if_sid>
475   <match>Connection reset</match>
476   <description>sshd: connection reset</description>
477 </rule>
478
479 <rule id="5763" level="10" frequency="8" timeframe="120" ignore="60">
480   <if_matched_sid>5760</if_matched_sid>
481   <same_source_ip/>
482   <description>sshd: brute force trying to get access to the system. Authentication failed.</description>
483   <mitre>
484     <id>T1110</id>
485   </mitre>
486   <group>authentication_failures,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_SI.4,nist_800_53_AU.14,nist_800_53_AC.7,pci_dss_11.4,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
487 </rule>
```

Riavvio il manager di **Wazuh** per applicare le modifiche.
Verifico poi che sull'agent dell'endpoint ci sia lo script per far *droppare* i pacchetti al firewall in caso di attacco brute force ssh:

```
root@Rosario:/home/vboxuser# cd /var/ossec/active-response/bin
root@Rosario:/var/ossec/active-response/bin# ls
default-firewall-drop  firewall-drop  ipfw          npf           restart-wazuh
disable-account        host-deny     kaspersky    pf           route-null
firewalld-drop        ip-customblock kaspersky.py restart.sh    wazuh-slack
root@Rosario:/var/ossec/active-response/bin#
```








ora che ho predisposto il manager e l'agent di **Wazuh** posso lanciare un attacco brute force tramite **Kali Linux** e il programma **Hydra**:

```
(kali㉿kali)-[~/home]
└─$ hydra -t 4 -l root -P /usr/share/wordlists/rockyou.txt 192.168.1.11 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-06 11:20:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.11:22/
```

Come possiamo notare dalla dashboard di **Wazuh** viene prima *triggerata* la regola che rileva l'attacco brute force e subito dopo viene attivato lo script sull'endpoint (host blocked by firewall-drop) per bloccare il tentativo di attacco brute force.

	Dec 6, 2024 @ 17:24:27.947	002	ubuntucione	T1110.001	Credential AccessLateral Move...	sshd: authentication failed.	5	5760
	Dec 6, 2024 @ 17:24:27.102	002	ubuntucione			Host Blocked by firewall-drop ...	3	651
	Dec 6, 2024 @ 17:24:25.998	002	ubuntucione	T1110.001	Credential AccessLateral Move...	sshd: authentication failed.	5	5760
	Dec 6, 2024 @ 17:24:25.948	002	ubuntucione	T1110.001	Credential AccessLateral Move...	sshd: authentication failed.	5	5760
	Dec 6, 2024 @ 17:24:25.944	002	ubuntucione	T1110	Credential Access	sshd: brute force trying to get ...	10	5763
	Dec 6, 2024 @ 17:24:23.986	002	ubuntucione	T1110.001	Credential AccessLateral Move...	sshd: authentication failed.	5	5760
	Dec 6, 2024 @ 17:24:23.986	002	ubuntucione	T1110.001	Credential AccessLateral Move...	sshd: authentication failed.	5	5760

W.

Rules

Rules (76)

From here you can manage your rules.

ssh

ID ↑	Description
5761	sshd: ssh connection closed.
5762	sshd: connection reset
5763	sshd: brute force trying to get access to the system.

sshd: brute force trying to get access to the system.

Authentication failed.

Information

ID	Level	File	Path
5763	10	0095-sshd_rules.xml	ruleset/rules

Groups
authentication_failures, syslog, sshd

Details