

PROJET : BLOCAGE DE COMPTES STAGIAIRES NON AUTORISÉS AVEC L'EDR (*Endpoint Detection and Response*) WAZUH



CONTEXTE

Dans ce projet nous allons bloquer la connexion en SSH (sur un ordinateur non autorisé) de 2 comptes utilisateurs qui appartiennent à deux stagiaires en Ressources humaines et en Comptabilité.

Dans un premier temps nous allons détecter les connexions en SSH des stagiaires et dans un deuxième temps nous allons créer une règle qui va bloquer la connexion après détection avec le module “ ACTIVE RESPONSE “de l' EDR WAZUH.

PARTIE 1 : CRÉATION DES COMPTES STAGIAIRES

Nous créons 2 comptes utilisateurs pour chaque stagiaire :

-Le stagiaire en Ressources Humaines aura comme identifiants :

Login= stagiaire-rh

Password=*****

-Le stagiaire en Comptabilité aura comme identifiants :

Login= stagiaire-compta

Password=*****


```
root@mdiaw: /home/mdiaw
root@mdiaw:/home/mdiaw# adduser stagiaire-rh
Adding user `stagiaire-rh' ...
Adding new group `stagiaire-rh' (1002) ...
Adding new user `stagiaire-rh' (1002) with group `stagiaire-rh' ...
Creating home directory `/home/stagiaire-rh' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for stagiaire-rh
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
root@mdiaw:/home/mdiaw#
```

```
root@mdiaw: /home/mdiaw
root@mdiaw:/home/mdiaw# adduser stagiaire-compta
Adding user `stagiaire-compta' ...
Adding new group `stagiaire-compta' (1003) ...
Adding new user `stagiaire-compta' (1003) with group `stagiaire-compta' ...
Creating home directory `/home/stagiaire-compta' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for stagiaire-compta
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
root@mdiaw:/home/mdiaw#
```

PARTIE 2 : CRÉATION DE CBD LISTS (Liste de contrôle d'accès)

Nous allons créer une liste dans le module CDB list (constant database) de Wazuh. Nous ajouterons dans cette liste les 2 stagiaires dont nous souhaitons bloquer la connexion.

De plus nous devons rajouter cette liste (Stagiaire-Non-Autorisés) dans le fichier **ossec.conf** de configuration de Wazuh pour qu'elle soit prise en compte.

 **W.** Settings

< Manager configuration

Edit **ossec.conf** of Manager

```
260 <localfile>
261   <log_format>full_command</log_format>
262   <command>last -n 20</command>
263   <frequency>360</frequency>
264 </localfile>
265
266 <ruleset>
267   <!-- Default ruleset -->
268   <decoder_dir>ruleset/decoders</decoder_dir>
269   <rule_dir>ruleset/rules</rule_dir>
270   <rule_exclude>0215-policy_rules.xml</rule_exclude>
271   <list>etc/lists/audit-keys</list>
272   <list>etc/lists/amazon/aws-eventnames</list>
273   <list>etc/lists/security-eventchannel</list>
274   <list>etc/lists/Test-List</list>
275   <list>etc/lists/Stagiaires-Non-Autorises</list>
276
277
278   <!-- User-defined ruleset -->
279   <decoder_dir>etc/decoders</decoder_dir>
280   <rule_dir>etc/rules</rule_dir>
281 </ruleset>
282
283 <rule_test>
284   <enabled>yes</enabled>
285   <threads>1</threads>
286   <max_sessions>64</max_sessions>
287   <session_timeout>15m</session_timeout>
```

PARTIE 3 : DÉTECTION DE CONNEXION DES STAGIAIRES.

Sur les images ci-dessous, nous pouvons constater que les connexions SSH des comptes stagiaires sont bien établies.

>	Aug 6, 2024 @ 11:47:56.084	PAM: Login session opened.	3	5501
>	Aug 6, 2024 @ 11:47:56.084	PAM: Login session opened.	3	5501
>	Aug 6, 2024 @ 11:47:56.057	sshd: authentication success.	3	5715

t	agent.ip	192.168.111.139
t	agent.name	mdiawlinux
t	data.dstuser	stagiaire-compta
t	data.srcip	192.168.111.136
t	data.srcport	52648
t	decoder.name	sshd
t	decoder.parent	sshd
t	full_log	Aug 6 11:47:55 mdiaw sshd[7573]: Accepted password for stagiaire-compta from 192.168.111.136 port 52648 ssh2
t	id	1722937676.62708
t	input.type	log
t	location	/var/log/auth.log
t	manager.name	wazuh-server
t	predecoder.hostname	mdiaw
t	predecoder.program_name	sshd
t	predecoder.timestamp	Aug 6 11:47:55
t	rule.description	sshd: authentication success.
#	rule.firedtimes	2

t agent.id	001
t agent.ip	192.168.111.139
t agent.name	mdiawlinux
t data.dstuser	stagiaire-rh
t data.srcip	192.168.111.136
t data.srcport	43922
t decoder.name	sshd
t decoder.parent	sshd
t full_log	Aug 6 11:47:40 mdiaw sshd[7254]: Accepted password for stagiaire-rh from 192.168.111.136 port 43922 ssh2
t id	1722937662.59750
t input.type	log
t location	/var/log/auth.log
t manager.name	wazuh-server
t predecoder.hostname	mdiaw
t predecoder.program_name	sshd
t predecoder.timestamp	Aug 6 11:47:40
t rule.description	sshd: authentication success.

PARTIE 4 : CRÉATION DE RÈGLE DE DÉTECTION LOCALE

Après avoir réussi la connexion en SSH des 2 comptes des stagiaires nous allons créer une règle de détection qui nous permettra de nous alerter lors de nouvelles connexions.

RÈGLE LOCALE ALERTE

<group name="Stagiaires-Non-Autorises">

<rule id="10024" level="11">

<if_sid>5715</if_sid>

<list field="user" lookup="match_key">etc/lists/Stagiaires-Non-Autorises </list>

**<description> DIAW-ADMIN a décidé de bloqué les stagiaires pour 600 secondes
!!!</description>**

</rule>

</group>

-EXPLICATION DE LA RÈGLE

group name = Nom de la liste des stagiaires à bloquer

rule id = Identifiant de la règle de détection (ici =10024)

if sid = Identifiant de la connexion en SSH pour Wazuh

list field= Chemin d'accès à la liste des stagiaires non autorisés à se connecter et vérification de la correspondance.

Description= Le message qui s'affiche lorsque les tentatives de connexion des stagiaires seront bloquées.

En résumé cette règle va tenter de détecter une connexion SSH de tous utilisateurs figurant sur la liste des stagiaires non autorisés à se connecter.

PARTIE 5 : CRÉATION DE RÈGLE DE BLOCAGE DE CONNEXION (AVEC ACTIVE RESPONSE) APRES DÉTECTION

Après la détection de la connexion des comptes stagiaires, nous devons mettre maintenant en place une règle qui interdit toute connexion des stagiaires en SSH.

Cette règle se met en place en utilisant le module ACTIVE RESPONSE de Wazuh.

ACTIVE RESPONSE

<active-response>

<command>firewall-drop</command>

<location>defined-agent</location>

<agent_id>001</agent_id>

<rules_id>10024</rules_id>

<timeout>600</timeout>

</active-response>

-EXPLICATION DE LA RÈGLE

<command>firewall-drop</command> = Bloque l'IP de l'utilisateur

<location>defined-agent</location> = Définition de l'agent wazuh qui se sera concerner lors de la tentative de connexion. Dans notre cas nous avons déployé un agent wazuh nommé *mdiawlinux* sur une machine UBUNTU.

<agent_id>001</agent_id> = Identifiant de l'agent wazuh *mdiawlinux* qui équivaut à 001.

<rules_id>10024</rules_id> = Identifiant de la règle ici 10024

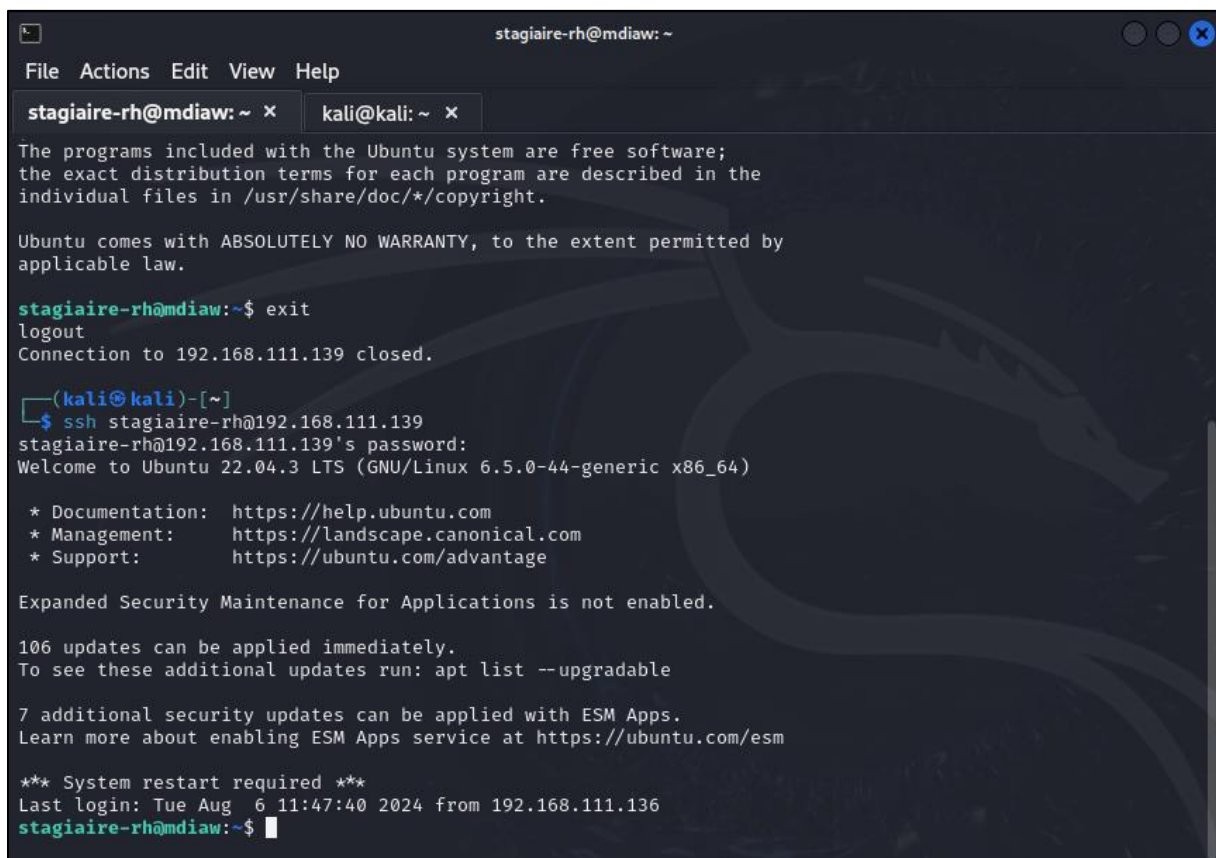
<timeout>600</timeout> = Durée pendant laquelle la connexion des stagiaires sera bloquée ici **600 secondes** = 10 minutes.

PARTIE 6 : VÉRIFICATION DU BLOCAGE DE LA CONNEXION DES STAGIAIRES

Après la création de la règle de détection et de blocage, les stagiaires tentent de se connecter en SSH sur la machine interdite portant l'adresse IP 192.168.111.139.

Après quelques tentatives, les stagiaires constatent qu'ils ne peuvent plus se connecter sur la machine 192.168.111.139.

Nous allons pousser notre investigation en nous connectant sur WAZUH afin de mieux comprendre ce qui s'est passé.



```
stagiaire-rh@mdiaw: ~
File Actions Edit View Help
stagiaire-rh@mdiaw: ~ x kali@kali: ~ x
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

stagiaire-rh@mdiaw:~$ exit
logout
Connection to 192.168.111.139 closed.

(kali@kali)-[~]
$ ssh stagiaire-rh@192.168.111.139
stagiaire-rh@192.168.111.139's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-44-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

106 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
Last login: Tue Aug  6 11:47:40 2024 from 192.168.111.136
stagiaire-rh@mdiaw:~$
```



```
stagiaire-compta@mdiaw: ~  
File Actions Edit View Help  
kali@kali: ~ x stagiaire-compta@mdiaw: ~ x  
$ ssh stagiaire-compta@192.168.111.139  
^C  
(kali@kali)-[~]  
$ ssh stagiaire-compta@192.168.111.139  
ssh: connect to host 192.168.111.139 port 22: Connection timed out  
(kali@kali)-[~]  
$  
(kali@kali)-[~]  
$ ssh stagiaire-compta@192.168.111.139  
stagiaire-compta@192.168.111.139's password:  
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-44-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Expanded Security Maintenance for Applications is not enabled.  
  
108 updates can be applied immediately.  
2 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
7 additional security updates can be applied with ESM Apps.  
Learn more about enabling ESM Apps service at https://ubuntu.com/esm  
  
*** System restart required ***  
Last login: Tue Aug  6 11:47:56 2024 from 192.168.111.136  
stagiaire-compta@mdiaw:~$
```

INVESTIGATION SUR WAZUH

Une fois connecté sur WAZUH nous détenons plus d'informations concernant l'échec de la tentative de connexion des stagiaires sur la machine **192.168.111.139**.

Nous pouvons lire sur les captures ci-dessous un message qui indiquent que l'hôte a été bloqué par la règle ACTIVE-RESPONSE que nous avons créé dans la partie 5.

La deuxième capture nous donne plus de détails sur ce blocage. Nous pouvons voir que l'utilisateur bloqué est bien le stagiaire en RH qui essaye de se connecter avec l'adresse IP **192.168.111.138**.

Nous pouvons aussi lire le message que nous avons spécifié lors de la création de la règle qui indique que l'administrateur a bloqué les stagiaires pour 600 secondes.

NB : Même interprétation pour le stagiaire en comptabilité

Security Alerts					
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Aug 6, 2024 @ 13:03:19.610			Host Blocked by firewall-drop Active Response	3	651
> Aug 6, 2024 @ 13:03:19.609			Apparmor DENIED	3	52002
> Aug 6, 2024 @ 13:03:19.499			Apparmor DENIED	3	52002
> Aug 6, 2024 @ 13:03:19.381	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> Aug 6, 2024 @ 13:03:19.365	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> Aug 6, 2024 @ 13:03:19.362			DIAW ADMIN a décidé de bloquer les stagiaires non autorisés pendant 600 secondes !!!	11	10024

t agent.name	mdiawlinux
t data.dstuser	stagiaire-rh
t data.srcip	192.168.111.136
t data.srcport	60716
t decoder.name	sshd
t decoder.parent	sshd
t full_log	Aug 6 13:03:18 mdiaw sshd[10620]: Accepted password for stagiaire-rh from 192.168.111.136 port 60716 ssh2
t id	1722942199.101556
t input.type	log
t location	/var/log/auth.log
t manager.name	wazuh-server
t predecoder.hostname	mdiaw
t predecoder.program_name	sshd
t predecoder.timestamp	Aug 6 13:03:18
t rule.description	DIAW ADMIN a décidé de bloquer les stagiaires non autorisés pendant 600 secondes !!!
# rule.firedtimes	1
t rule.groups	Stagiaires-Non-Autorises

Security Alerts					
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Aug 6, 2024 @ 13:18:04.315			Host Blocked by firewall-drop Active Response	3	651
> Aug 6, 2024 @ 13:18:02.630			Apparmor DENIED	3	52002
> Aug 6, 2024 @ 13:18:02.442			Apparmor DENIED	3	52002
data.parameters.alert.agent.name mdiawlinux					
data.parameters.alert.data.dstuser stagiaire-compta					
data.parameters.alert.data.srcip 192.168.111.136					
data.parameters.alert.data.srcport 59390					
data.parameters.alert.decoder.name sshd					
data.parameters.alert.decoder.parent sshd					
data.parameters.alert.full_log Aug 6 13:18:01 mdiaw sshd[11627]: Accepted password for stagiaire-compta from 192.168.111.136 port 59390 ssh2					
data.parameters.alert.id 1722943082.109909					
data.parameters.alert.location /var/log/auth.log					
data.parameters.alert.manager.name wazuh-server					
data.parameters.alert.predecoder.hostname mdiaw					
data.parameters.alert.predecoder.program_name sshd					
data.parameters.alert.predecoder.timestamp Aug 6 13:18:01					
data.parameters.alert.rule.description DIAW ADMIN a décidé de bloquer les stagiaires non autorisés pendant 600 secondes !!!					
data.parameters.alert.rule.firedtimes 2					

ANNEXES

