Ecole Nationale des Sciences Appliquées de Sciences Appliquées de Khouribga

Filière : Ingénierie des Réseaux Intelligents &Cybersécurité

Rapport du Mini Projet:

Évaluation Efficace du SOC avec MITRE ATT&CK

Réalisé par :

- **EL GHAIT Imane**
- **AMAOUI Imane**

Encadré par :

- **Mr MALEH Yassine**

Table des matières

Table des matières

Introduction

Le présent rapport est réalisé dans le cadre du mini-projet intitulé **"SOC Use Cases Basés sur MITRE ATT&CK",** issu du cours d'introduction à la cybersécurité. L'objectif principal de ce projet est de concevoir et d'implémenter des cas d'usage pour la détection d'activités suspectes dans un environnement SOC (Security Operations Center), en se basant sur les tactiques, techniques et procédures (TTPs) identifiées lors de l'opération "**Soft Cell".**

Ce projet s'appuie sur l'utilisation de la plateforme Wazuh pour configurer des règles de détection permettant de surveiller des comportements malveillants spécifiques, alignés avec les techniques du **Framework MITRE ATT&CK**. À travers une démarche structurée, nous explorons des phases telles que l'accès initial, la persistance, le déplacement latéral et le dumping d'identifiants. Les objectifs sont d'améliorer la sécurité proactive d'un SOC et de renforcer la capacité de réponse en temps réel face aux cybermenaces.

Les résultats escomptés incluent une meilleure compréhension des **TTPs**, une configuration efficace des règles de détection, ainsi que des recommandations concrètes pour l'optimisation des capacités de détection du SOC.

Etape 1 : Analyse de l'Étude de Cas et Identification des TTPs :

D'après l'analyse du Rapport de la compagne « Operation Soft Cell », on a observé des Tactiques et techniques avec le Framework MITRE ATT&CK :

THE ATTACK

The initial indicator that 'sparked our imagination' was malicious activity performed by w3wp.exe, an IIS process, which was eventually classified as a webshell activity. By investigating the webshell

(which was later classified as the 'China Chopper' [1, 2] webshell), we were able to unravel several attack phases and TTPs used by the attackers.

The attackers leveraged the webshell to run reconnaissance commands and credential-stealing activities.

One of the reconnaissance actions was to run a modified *NirSoft* NetBIOS scanner in order to identify available NetBIOS name servers locally or over the network.

The credential-stealing tool was a modified Mimikatz version, which, when executed, only dumps NTLM hashes (note that it does not require any command line arguments). We renamed this sample maybemimi.exe.

Reverse engineering shows the string similarity between maybemimi.exe and Mimikatz, as shown in Figures 5 and 6.

emerging, as well as reconnaissance and credential-stealing activity. In addition, we uncovered the usage of PiVy (Poison Ivy) by the attackers.

PiVy

Poison Ivy (or PiVy for short) is a RAT that is associated with Chinese threat actors. PiVy is a powerful, well-featured RAT that allows an attacker to take total control of a machine. Among its containment actions that, later on, were put in place on an ad-hoc basis. We kept track in our research of the different TTPs of the threat actor, and there were no new indicators until the end of 2018. During that time, we detected interesting compressing activity carried out by the attackers in order to exfiltrate data. The attackers used *WinRAR*, which they downloaded from their C2 server, to compress the data they wanted to steal. By leveraging (another) webshell, and a renamed cmd.exe version, the attackers executed reconnaissance commands, collected data, dropped tools like portqry.exe and hTran, and performed lateral movement using `net use` and wmic.exe.

hTran

One of the tools that the attackers deployed in order to exfiltrate the data from network segments that were not connected to the Internet was a customized version of hTran, a 'connection bouncer' tool which allows the attacker to redirect ports and connections between different networks. hTran's code is publicly available on *GitHub* [4].

Tactics	ID	Techniques	ID	Description (objectif des attaquants)
Persistance	T1505	-Webshells	T1505.003	Les attaquants ont utilisé des webshells, comme "China Chopper," pour obtenir un accès initial aux systèmes compromis.
		-Remote Access Trojan	T1219	-Poison Ivy (PiVy) a été installé en tant que RAT (Remote Access Trojan) persistant avec des fonctionnalités avancées
Credential Access	TA0006	-OS Credential Dumping LSASS Memory	T1003	Utilisation de versions modifiées d'outils comme Mimikatz (nommé "maybemimi.exe") pour récupérer des hash NTLM et d'autres informations d'identifiants.
Reconnaissance	TA0043	- Network Service Scanning	T1046	Les attaquants ont utilisé des outils comme un scanner NetBIOS de NirSoft pour explorer le réseau, identifier les serveurs de noms et obtenir une cartographie des ressources locales et distantes.
		- System Network Connections Discovery	T1049	
		- System Network Configuration Discovery	T1016	
		-Remote System Discovery	T1018	
Execution	TA0002	-Command and Scripting Interpreter	T1059	Des webshells ont été utilisés pour exécuter des commandes directement sur les serveurs compromis. - Windows Command Shell <<<cmd.exe
Defense Evasion	TA0005	- DLL via Side-Loading.	T1574.002	-Les attaquants ont utilisé des logiciels signés et légitimes (comme des outils Samsung) pour charger des DLL malveillantes et éviter la détection. -les attaquants ont modifié les noms et les chaînes de caractères des outils pour échapper à la détection. Mimikatz vers "maybemimi.exe"
		- Signed Binary Proxy Execution	T1218	
		-Obfuscation	T1027	
		-Masquerading	T1036	
Exfiltration	TA0010	- Archive Collected Data	T1560.001	- Les attaquants ont utilisé WinRAR pour compresser les fichiers avant de les exfiltrer. -Utilisation de l'outil hTran pour rediriger les connexions et exfiltrer
		-Non-Standard Port	T1048.003	

		-Exfiltration Over C2 Channel	T1041	des données depuis des segments de réseau isolés.
Command and Control		-Application Layer Protocol -Dynamic Resolution: Domain Generation Algorithms	T1071.001 T1568.002	
Collection	TA0009	-Input Capture: Keylogging -Data from Information Repositories CDR	T1056.001 T1213.001	Keylogging and various other surveillance features -One of the most valuable pieces of data that telcos hold are CDRs – call detail records. CDRs are basically a large subset of metadata containing all the details about calls
Lateral Movement	TA0008	- Remote Services: SMB/Windows Admin Shares	T1021.002	CDRversion, the attackers executed reconnaissance commands, collected data, dropped tools like portqry.exe and hTran, and performed lateral movement using `net use` and wmic.exe

Etape 2 : Définition des SOC Use Cases Basés sur les TTPs :

Intégrer MITRE ATT&CK dans un **SOC (Security Operations Center)** pour améliorer la détection et la réponse aux incidents de sécurité.

Pour chaque TTP identifié, définir un use case de détection dans le contexte SOC et l'objectif de détection et les déclencheurs spécifiques à surveiller.

Use Case	TTP(Technique)	MITTRE ATT&CK ID	Objectif de détection
Détecter des webshells	Webshell	T1505.003	Détecter l'activité anormale associée à des webshells : commandes exécutées via des processus inattendus (ex : w3wp.exe pour IIS).
Accès Persistant avec RAT	Remote Access Trojan	T1219	Identifier l'utilisation continue des outils RAT comme Poison Ivy pour maintenir un contrôle à long terme sur les systèmes compromis, en surveillant les communications régulières avec les serveurs de commande et de contrôle (C2).

Détecter l'utilisation de credentiel dumping ou d'outils connus, même s'ils sont modifiés ou masqués.	OS Credential Dumping	T1003	Détecter l'activité des attaquants pour extraire les identifiants et les hash de mots de passe stockés dans le système d'exploitation. Les outils comme Mimikatz vers maybemimi.exe
Identifier et bloquer les scans réseau effectués par des attaquants	Network Service Scanning	T1046	
Découverte des connexions réseau système	System Network Connections Discovery	T1016	Identifier les requêtes inhabituelles ou répétées sur des segments réseau spécifiques, notamment via des outils comme NetBIOS scanner ou commandes PowerShell.
Découverte de la configuration réseau système	- System Network Configuration Discovery	T1016	. Identifier l'exécution de commandes ou d'outils visant à collecter des informations sur la configuration réseau, comme l'utilisation de ipconfig, route ou d'autres utilitaires systèmes.
Commandes et scripts interprétés	Command and Scripting Interpreter	T1059	Détecter les commandes encodées ou masquées (ex. : Encoded Command dans PowerShell), utilisées pour échapper aux systèmes de détection classiques
-Découverte de systèmes distants	Remote System Discovery	T1018	Identifier les tentatives de reconnaissance sur des hôtes distants en surveillant des outils tels que net use et wmic.exe.
Détecter et bloquer les RATs	Remote Access Trojan (RAT)	T1219	Détecter les comportements malveillants liés à l'exécution ou au contrôle à distance.
-DLL via Side-Loading	DLL Side-Loading	T1574.002	Identifier les tentatives de chargement de DLL non autorisées ou malveillantes via des applications légitimes.
Archivage des données dans des formats standards (.zip .rar.tar ….)	Archive Collected Data	T1560.001	Détection des fichiers d'archives inhabituels
-Utilisation de protocoles d'application pour exfiltration	-Obfuscation Application Layer Protocol	T1027	Identifier les outils ou fichiers malveillants déguisés par modification de chaînes ou d'attributs (ex. changement des noms de fichiers).
Résolution dynamique avec des algorithmes de génération de domaine	Dynamic Resolution: Domain Generation Algorithms	T1568.002	Détecter les requêtes DNS vers des domaines générés dynamiquement (par exemple, via des algorithmes de génération de domaine - DGA)
Exfiltration de données via C2	Exfiltration Over C2 Channel	T1041	Détecter les activités de transfert de données volumineuses ou continues vers des domaines ou IPs suspects liés

			aux C2, en utilisant des outils comme hTran.
Exécution par proxy avec des binaires signés	Signed Binary Proxy Exécution	T1218	Détecter l'utilisation de binaires signés légitimes (comme RunHelp.exe) pour charger des bibliothèques malveillantes (DLL side-loading)

Etape 3: Création des Règles de Détection dans Wazuh

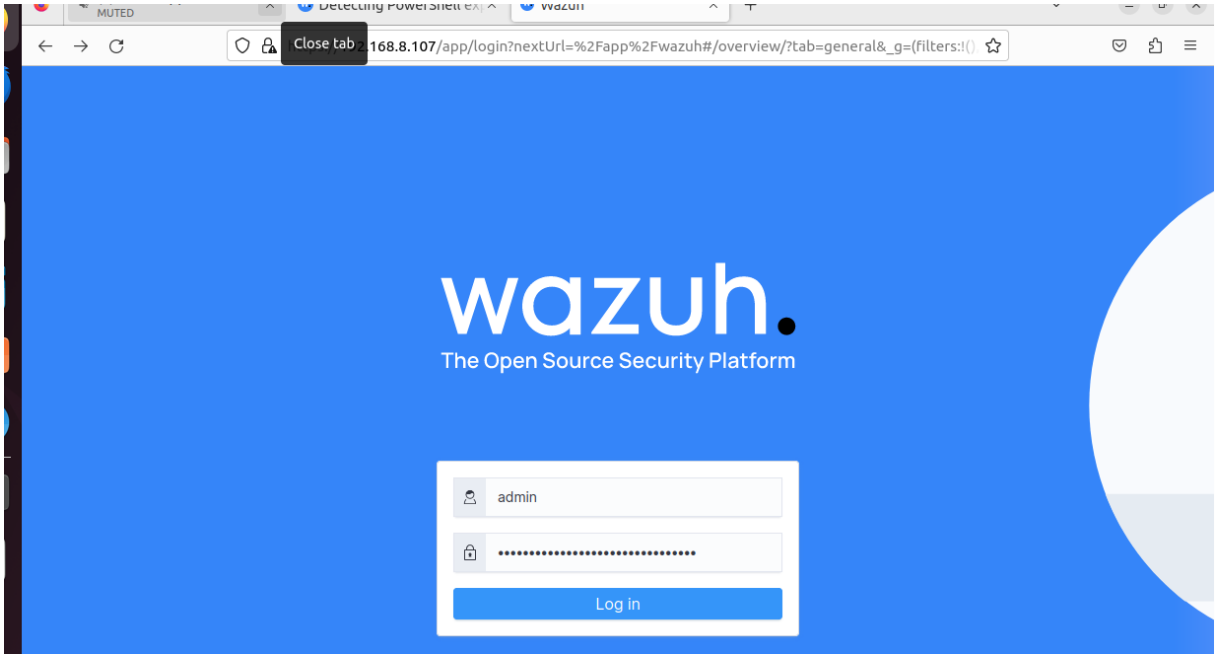
Installation Wazuh sur la VM :

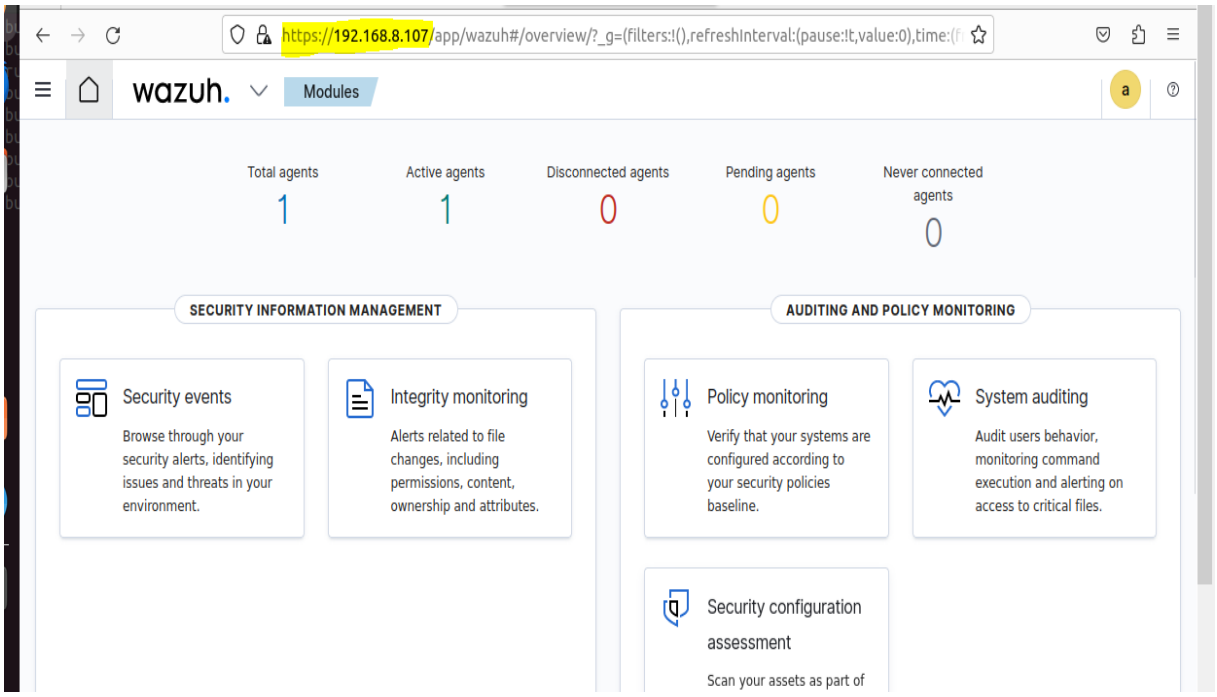
```
$ curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-i
nstall.sh -a
```

```
10.0.2.15           38          96  21    0.57    0.62     0.64 dimr      cluster_manager,data,ingest,remote_cluster_client *
        node-1
root@ubuntu:/home/imane/Desktop#  apt-get -y install wazuh-manager
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wazuh-manager is already the newest version (4.9.2-1).
0 upgraded, 0 newly installed, 0 to remove and 341 not upgraded.
root@ubuntu:/home/imane/Desktop# systemctl daemon-reload
root@ubuntu:/home/imane/Desktop# systemctl enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service -> /lib/systemd/system/wazuh-manager.service.
root@ubuntu:/home/imane/Desktop# systemctl start wazuh-manager
root@ubuntu:/home/imane/Desktop# systemctl status wazuh-manager
* wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; >
     Active: active (running) since Thu 2024-11-14 20:28:50 +01; 57min ago
      Tasks: 101 (limit: 4753)
     Memory: 288.6M
        CPU: 2min 59.787s
     CGroup: /system.slice/wazuh-manager.service
             |-63583 /var/ossec/framework/python/bin/python3 /var/ossec/a>
             |-63623 /var/ossec/bin/wazuh-authd
             |-63639 /var/ossec/bin/wazuh-db
             |-63663 /var/ossec/bin/wazuh-execd
             |-63667 /var/ossec/framework/python/bin/python3 /var/ossec/a>
```

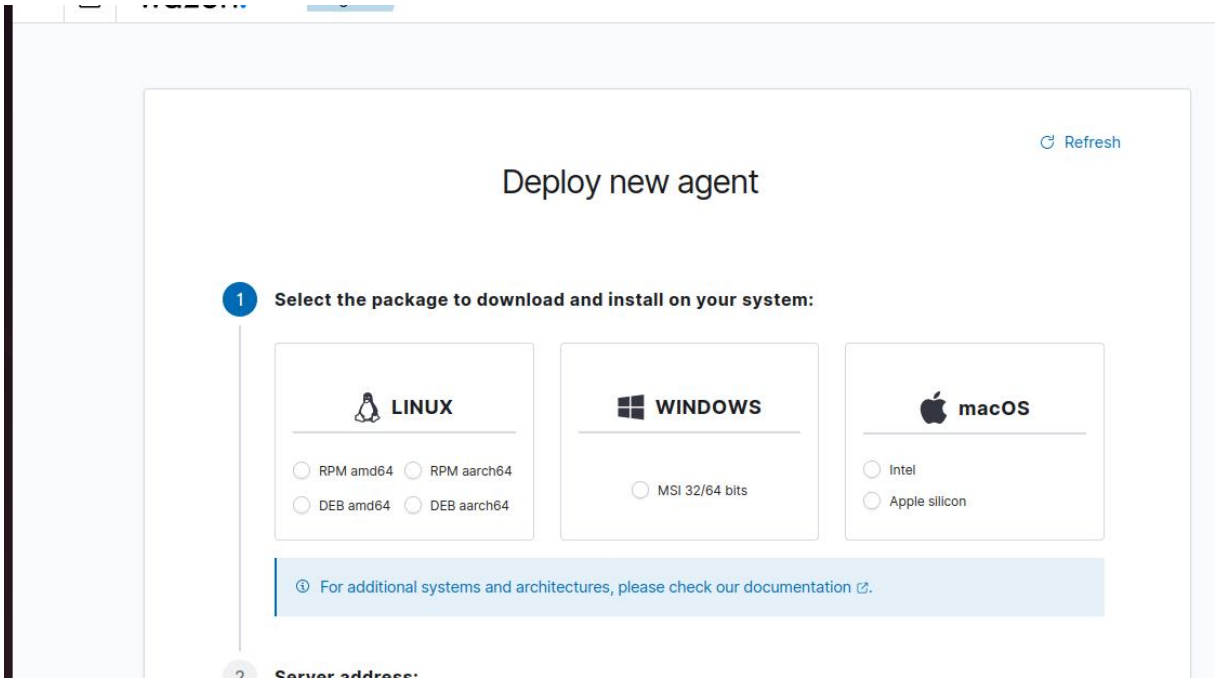
```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

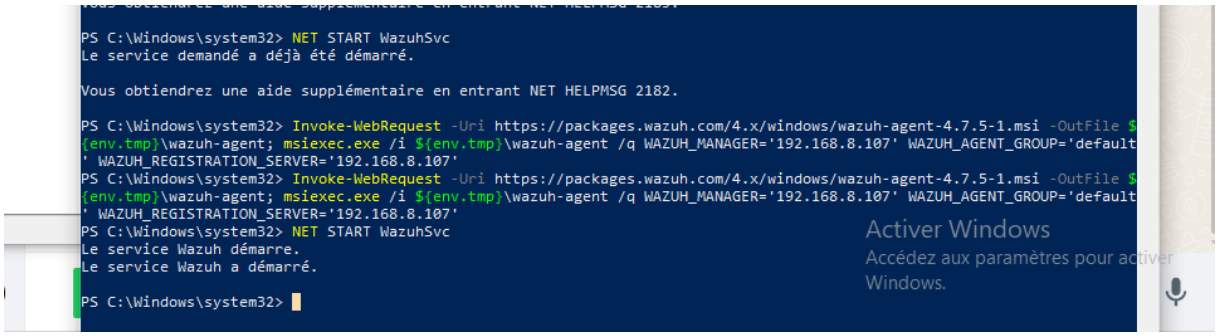
Access the Wazuh web interface with https://192.168.8.107 and your credentials:

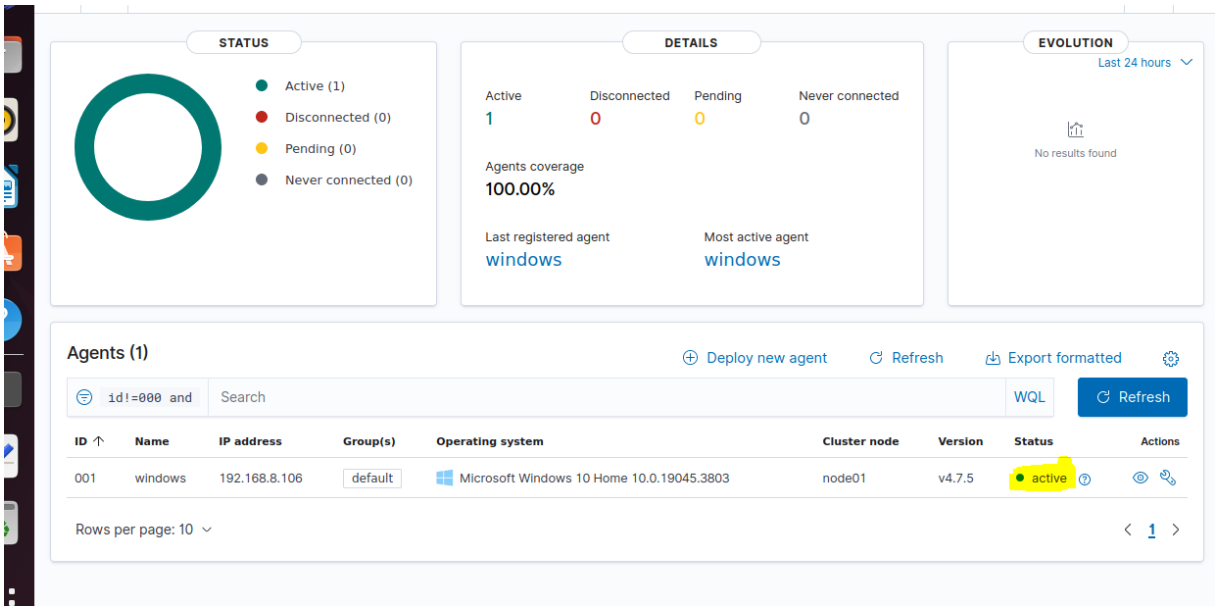




Ajout de l’agent : Windows 10 : IP :192.168.8.106





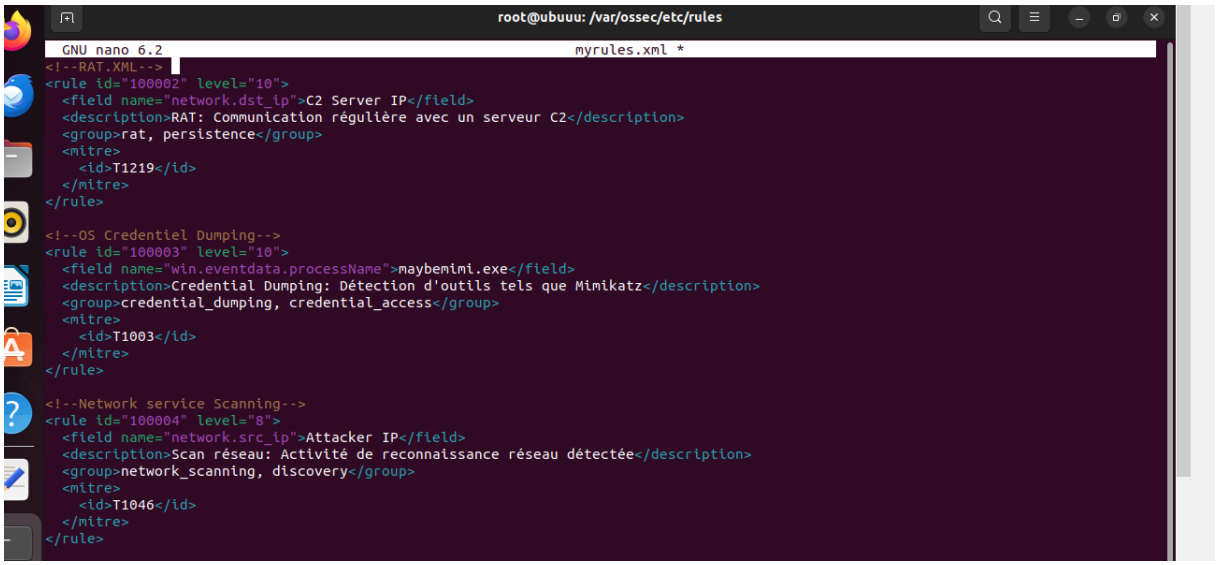


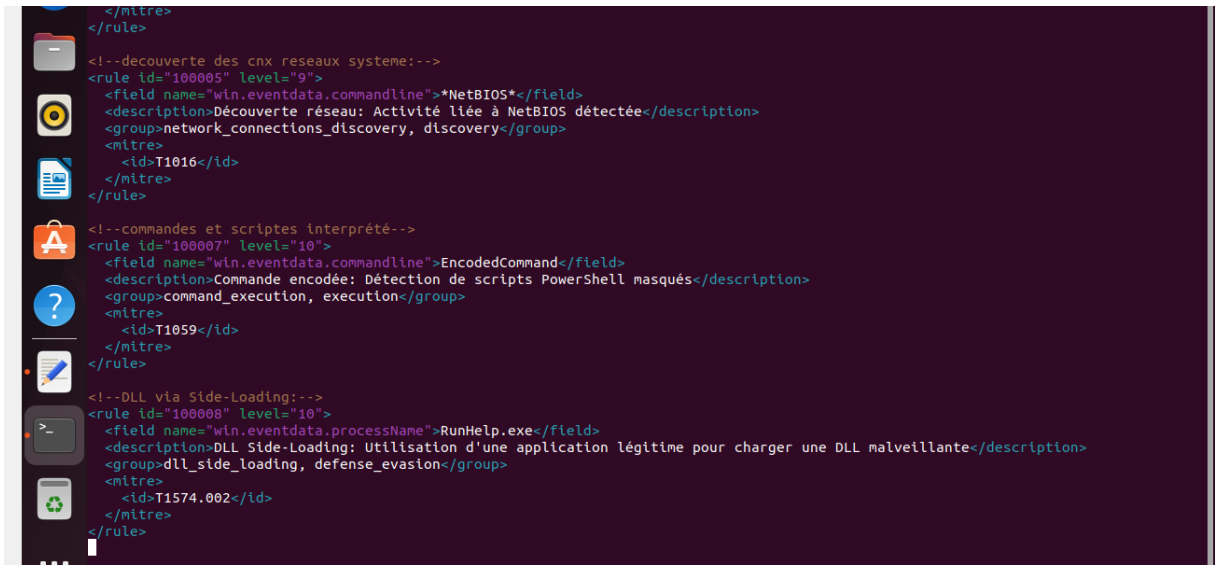
Configuration des règles de Détection en ciblant le comportement des TTPs identifiés :

Chaque Règle de Détection compris :

- ID de la règle
- Niveau de criticité (de 0 jusqu'à 10)
- Logique de détection
- La tactique et la technique dont elle appartient

Création d'un fichier **/var/ossec/etc/rules/myrules.xml** dont lequel on ajoutera les règles de détections en se basant sur les uses cases des TTPs identifiées :



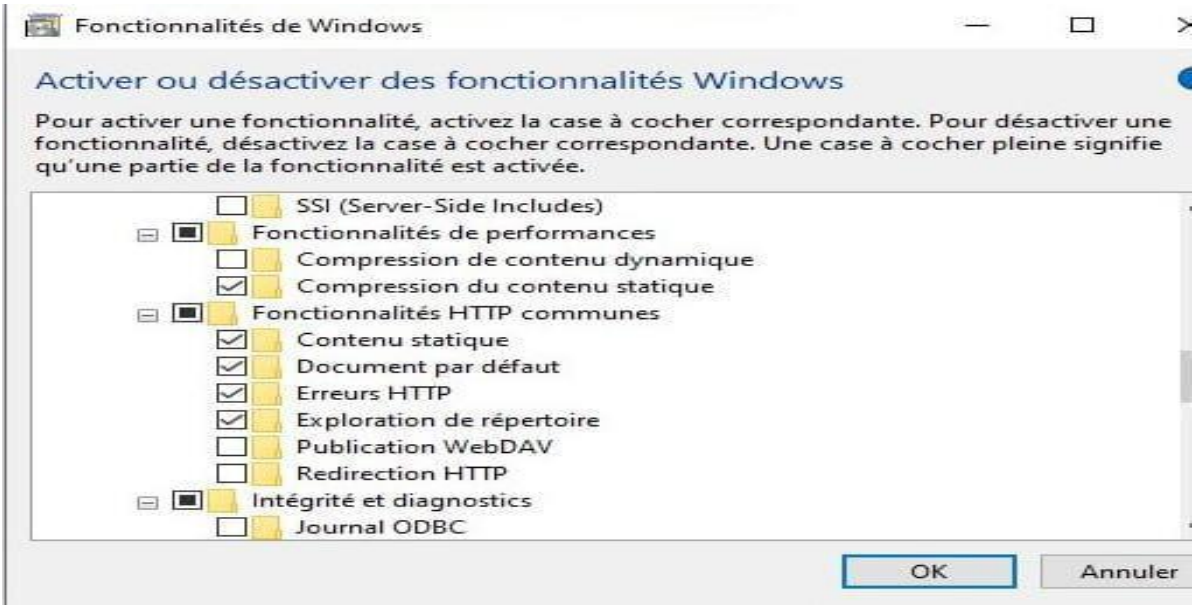


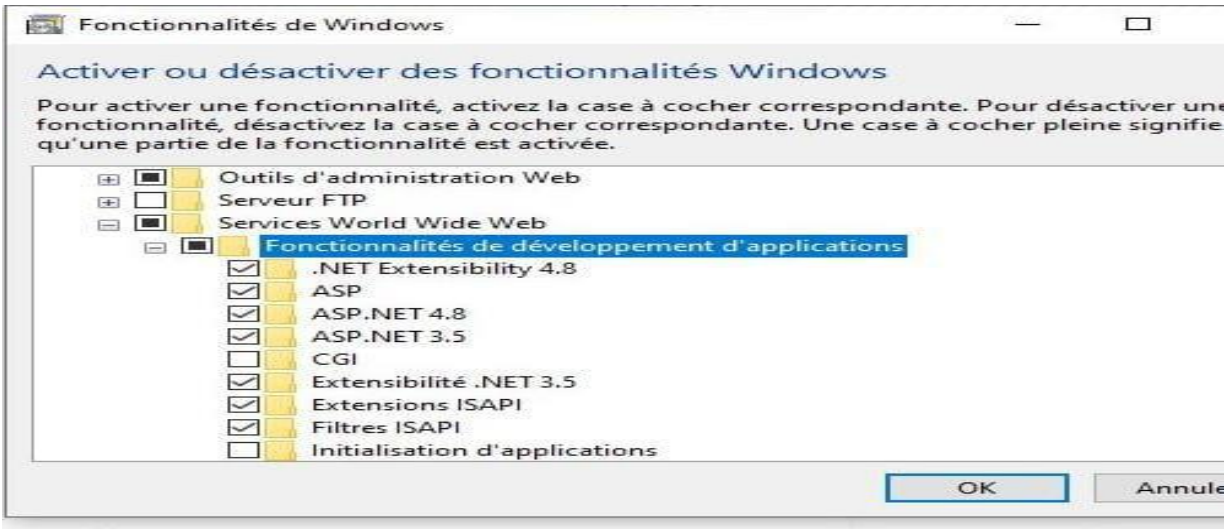
Et Redémarrer le service Wazuh-manager :

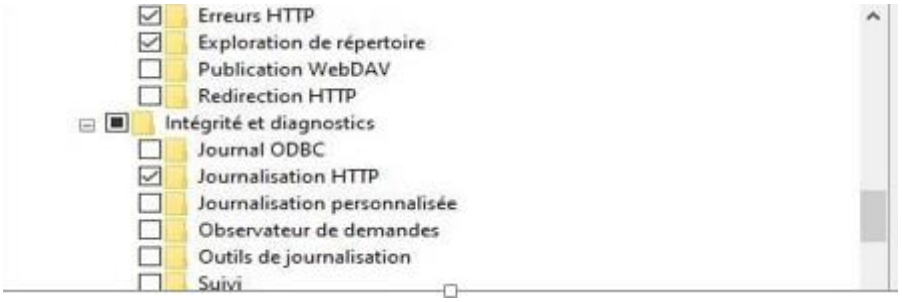
```
root@ubuuu:/var/ossec/etc/rules# sudo systemctl restart wazuh-manager
root@ubuuu:/var/ossec/etc/rules# ls
```

Use Case 1 :Détection Webshell :

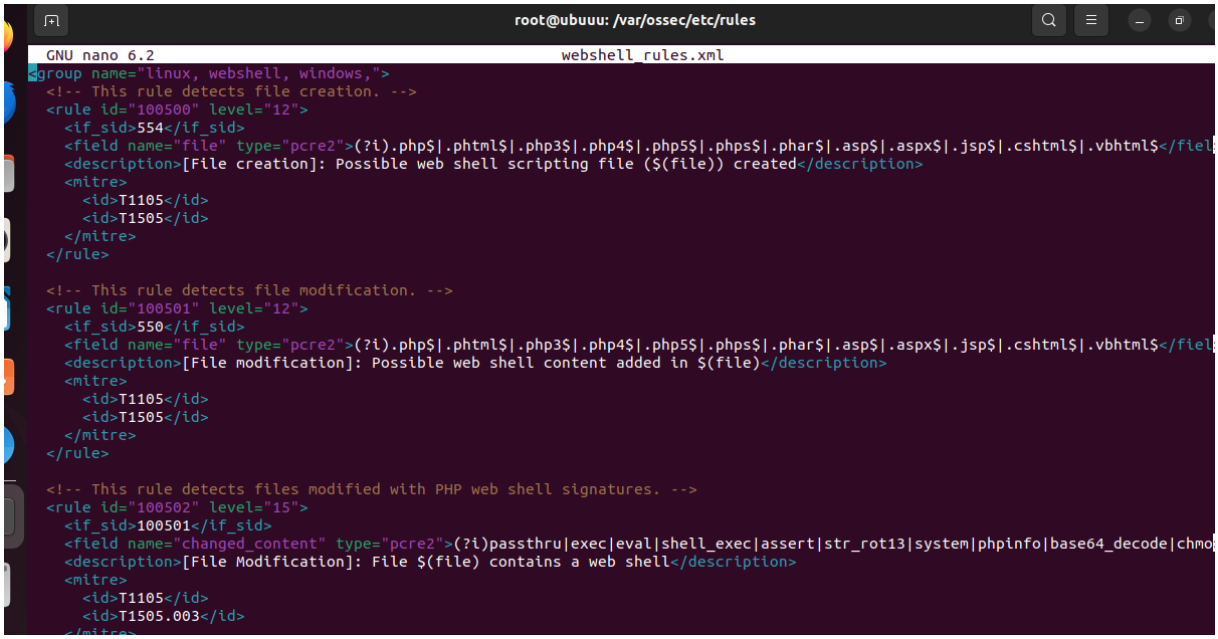
Configuration de **IIS web server** on the Windows Agent :







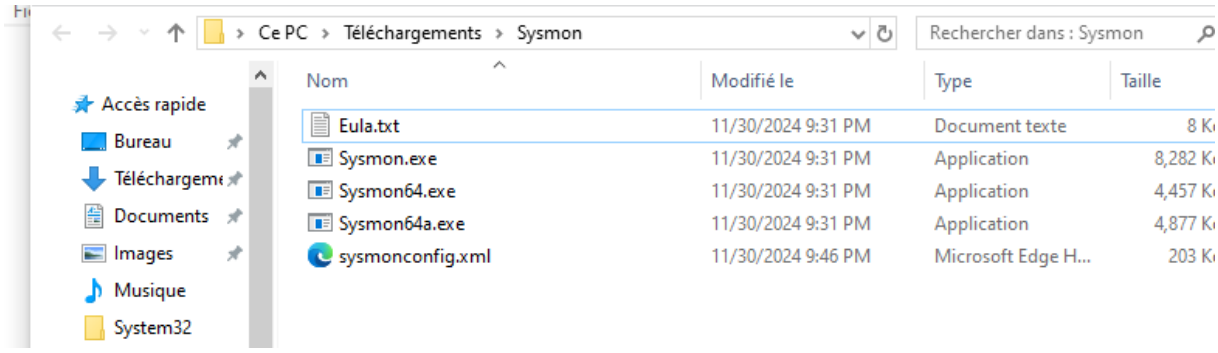
Ajouter la règle : Dans le fichier webshell_rules.xml

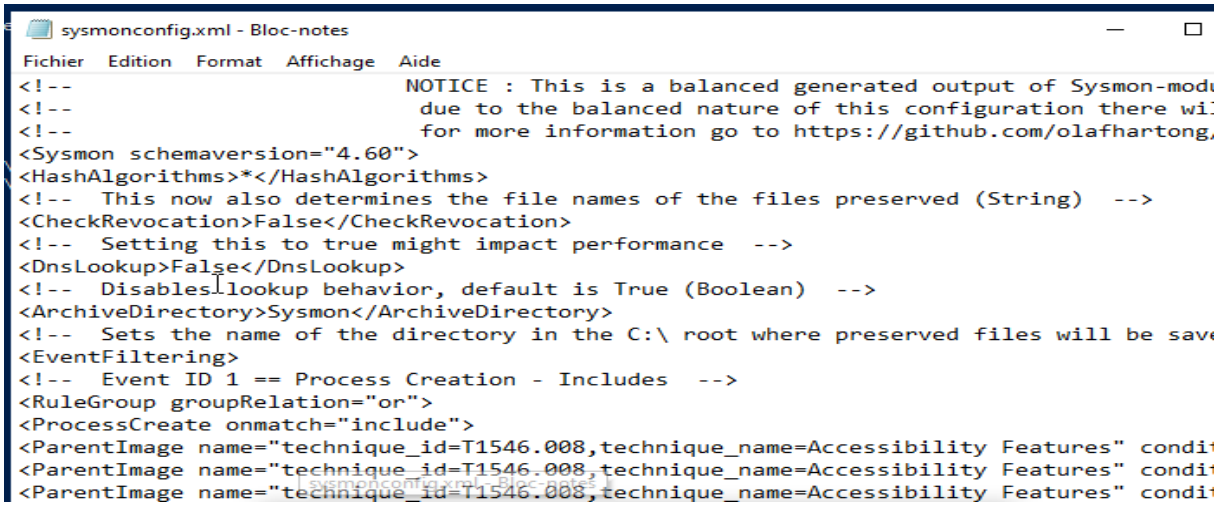


Et Redémarrer le service Wazuh Manager

```
systemctl restart wazuh-manager
```

Installation de Sysmon installer et configurer le fichier sysmonconfig.xml :

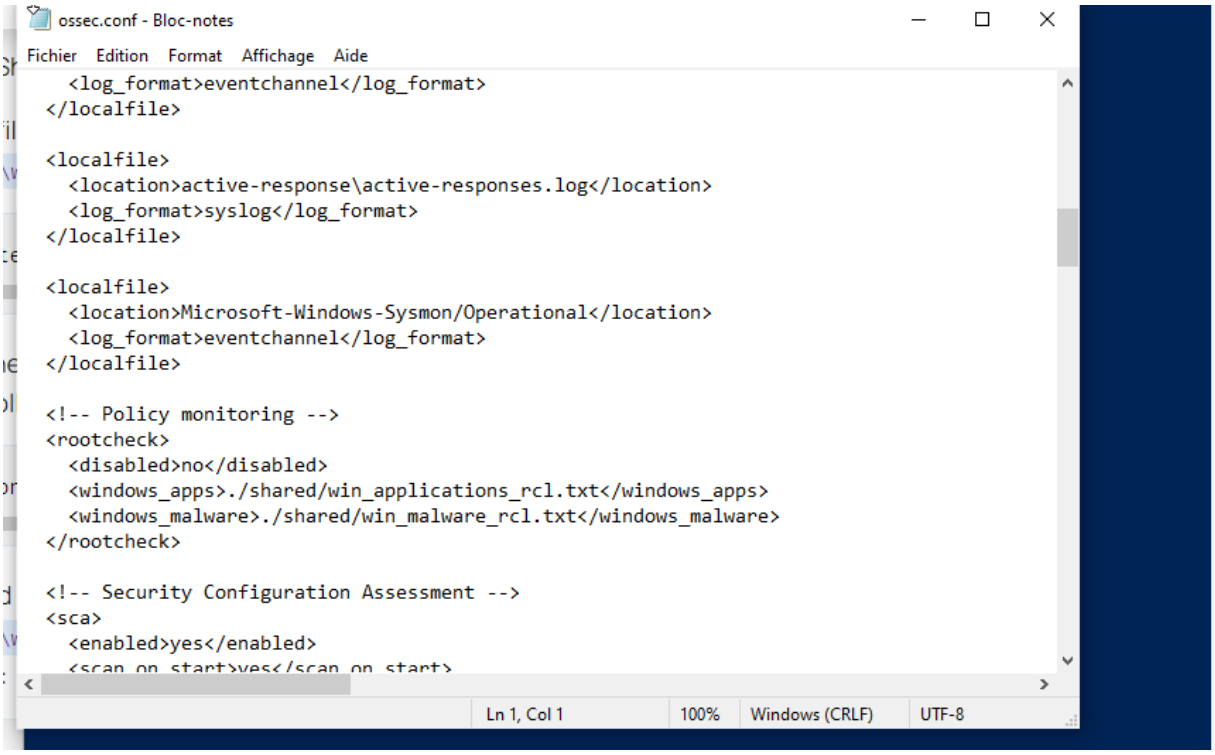




```
> .\Sysmon64.exe -accepteula -i sysmonconfig.xml
```

```
PS C:\> cd 'C:\Users\imanewin\Downloads'
PS C:\Users\imanewin\Downloads> cd 'Sysmon'
PS C:\Users\imanewin\Downloads\Sysmon> .\Sysmon64.exe -accepteula -i sysmonconfig.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.60
Sysmon schema version: 4.90
Configuration file validated.
The service Sysmon64 is already registered. Uninstall Sysmon before reinstalling.

PS C:\Users\imanewin\Downloads\Sysmon>
```

```
PS C:\Windows\system32> cd 'C:\Program Files (x86)\ossec-agent'
PS C:\Program Files (x86)\ossec-agent> notepad ossec.conf
PS C:\Program Files (x86)\ossec-agent>
```




```
Restart-Service -Name wazuh
```

- Ajouter dans le fichier webshell_rules.xml, les règles qui permettent de détection les commandes de web Shell d'exécution et d'établissement de connexion :

```
<!-- Windows Rules. -->
<group name="sysmon, webshell, windows,">
  <!-- This rule detects web shell command execution. -->
  <rule id="100530" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.parentImage" type="pcre2">(?i)w3wp\.exe</field>
    <field name="win.eventdata.parentUser" type="pcre2">(?i)IIS\sAPPPOOL\\\\DefaultAppPool</field>
    <description>[Command execution ($(win.eventdata.commandLine))]: Possible web shell attack detected</description>
    <mitre>
      <id>T1505.003</id>
      <id>T1059.004</id>
    </mitre>
  </rule>

  <!-- This rule detects web shell network connections. -->
  <rule id="100531" level="12">
    <if_sid>61605</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)w3wp\.exe</field>
    <field name="win.eventdata.user" type="pcre2">(?i)IIS\sAPPPOOL\\\\DefaultAppPool</field>
    <description>[Network connection]: Possible web shell attempting network connection on source port: $(win.eventdata.sourcePort)</description>
    <mitre>
      <id>TA0011</id>
      <id>T1049</id>
      <id>T1505.003</id>
    </mitre>
  </rule>
</group>
```

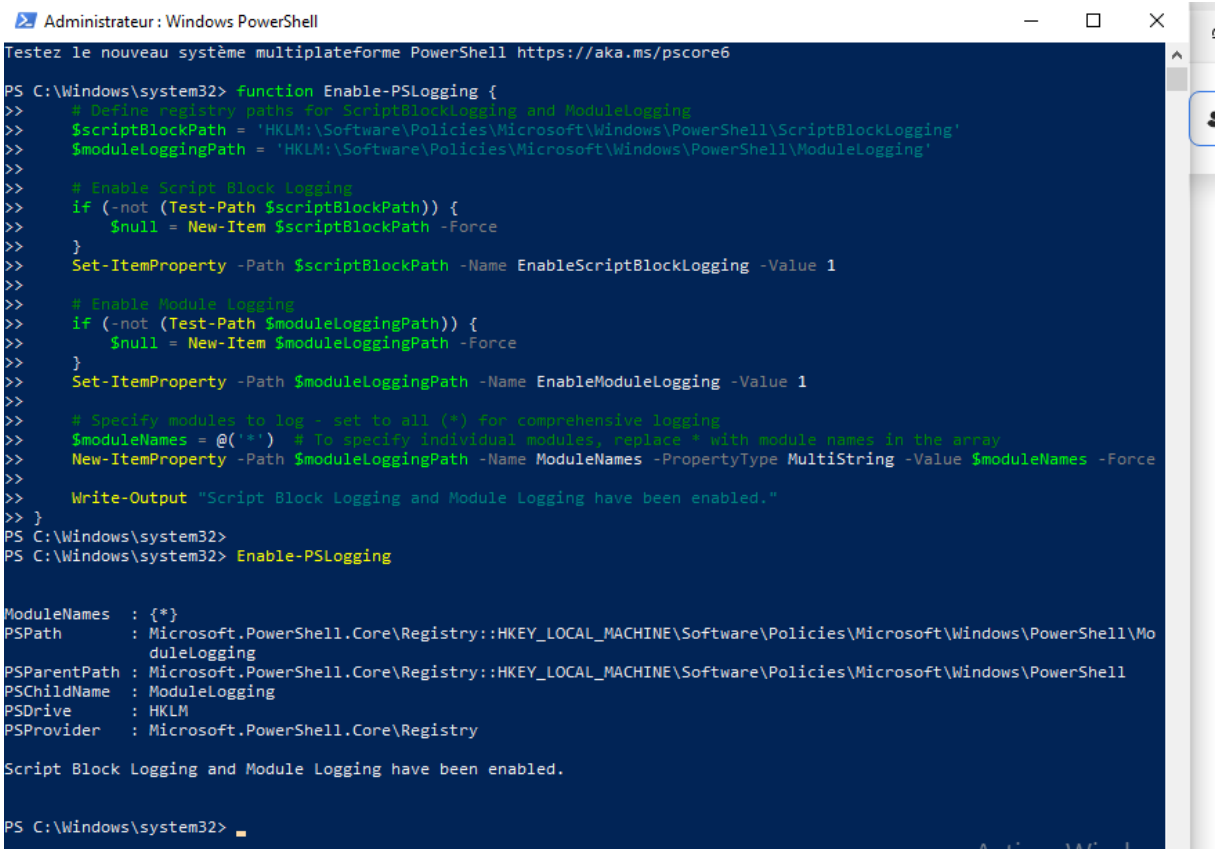
```
<!-- Linux Rules. -->
<group name="auditd, linux, webshell,">
  <!-- This rule detects web shell command execution. -->
  <rule id="100520" level="12">
    <if_sid>80700</if_sid>
    <field name="audit.key">webshell_command_exec</field>
    <description>[Command execution ($(audit.exe))]: Possible web shell attack detected</description>
    <mitre>
      <id>T1505.003</id>
      <id>T1059.004</id>
    </mitre>
  </rule>

  <!-- This rule detects web shell network connections. -->
  <rule id="100521" level="12">
    <if_sid>80700</if_sid>
    <field name="audit.key">webshell_net_connect</field>
    <description>[Network connection via $(audit.exe)]: Possible web shell attack detected</description>
    <mitre>
      <id>TA0011</id>
      <id>T1049</id>
      <id>T1505.003</id>
    </mitre>
  </rule>
```

Redémarrer le service wazuh-manager :

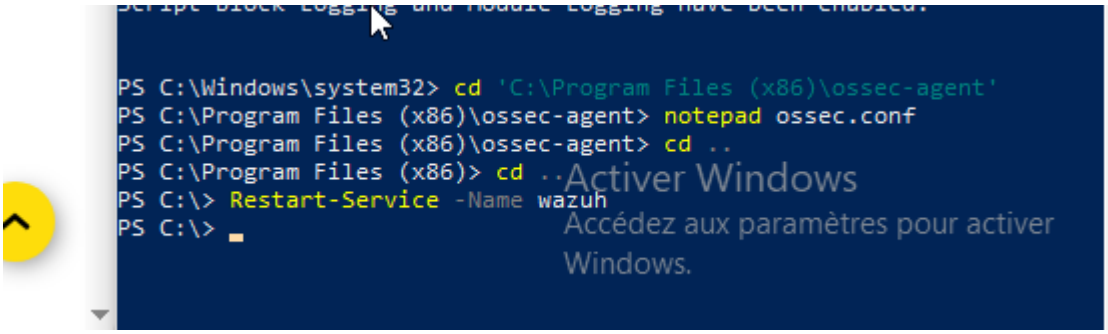
```
sudo systemctl restart wazuh-manager
```

Use Case : Détection PowerShell :

- Activation de la journalisation PowerShell pour avoir une journalisation détaillée dans PowerShell :
- Ouvrir Powershell en tant qu'administrateur :



Le transfert des journaux PowerShell au serveur Wazuh pour les analyser ce fait comme suit :



Ajouter les règles de détection dans le fichier **/var/ossec/etc/rules/local_rules.xml** :

Et Redémarrer le service Wazuh-manager :

```
systemctl restart wazuh-manager
```

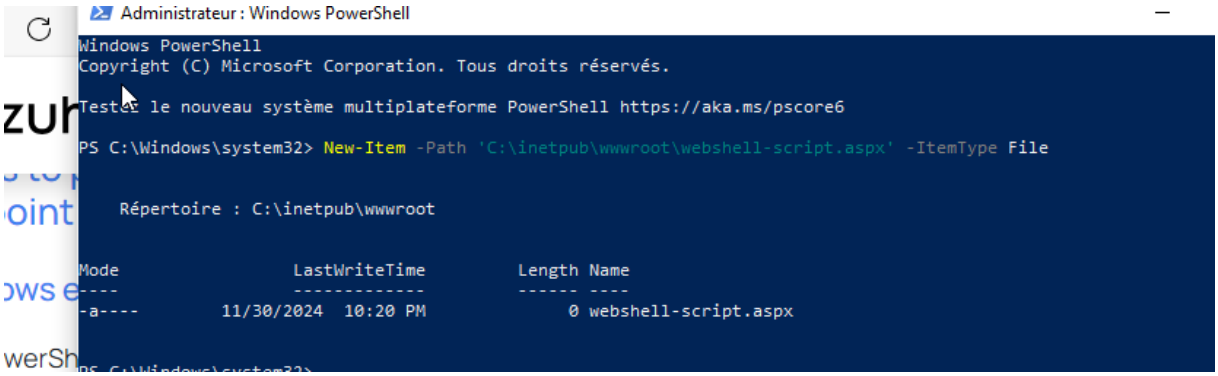
Etape 4 : Simulation des Use Cases et Validation des Alertes :

1-Use Case 1 : Détection WebShell :

Lancer le Power Shell au tant qu'Administrateur et exécuter la commande suivante :

1ere Attack :

- **Création d'un fichier dans le répertoire du serveur web : webshell-script.aspx C:\inetpub\wwwroot**



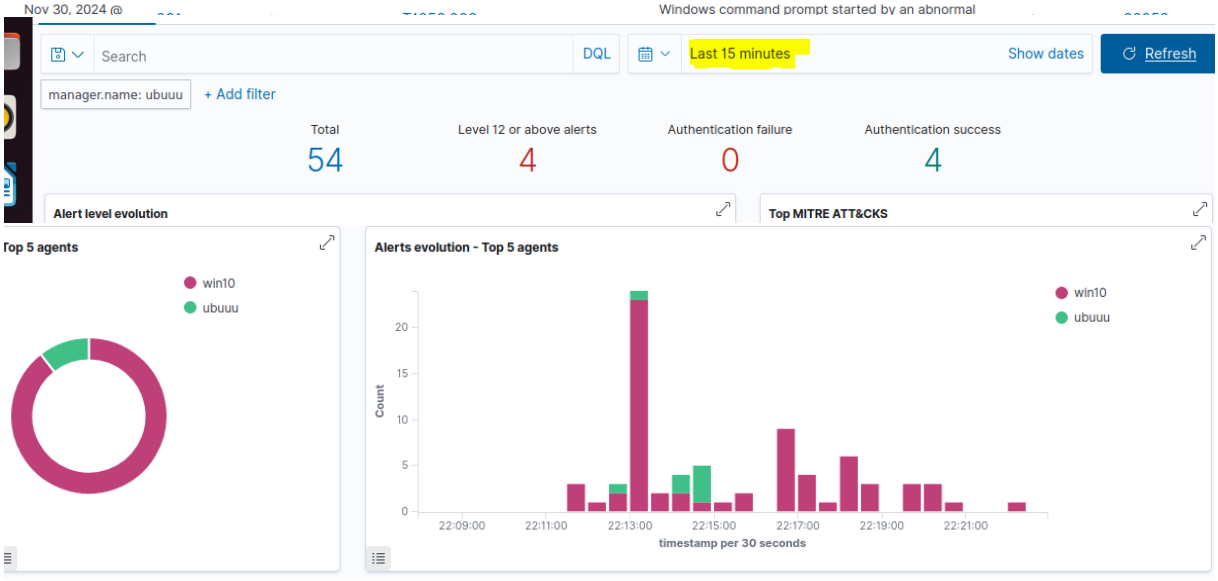
Accéder à l'interface du server Wazuh :

Security Events >Alertes : (pour les dernières 15 minutes)

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Nov 30, 2024 @ 22:24:58.031	001	win10	T1574.001 T1574.002	Persistence, Privilege Escalation, Defense Evasion	Possible DLL search order hijack by C:\\Windows \\SoftwareDistribution\\Download \\debd60358786516fd3e6fc91795ca227\\Metadata \\dpx.dll created in Windows root folder	6	92219
Nov 30, 2024 @ 22:24:57.984	001	win10	T1574.001 T1574.002	Persistence, Privilege Escalation, Defense Evasion	Possible DLL search order hijack by C:\\Windows \\SoftwareDistribution\\Download \\debd60358786516fd3e6fc91795ca227\\Metadata \\UpdateAgent.dll created in Windows root folder	6	92219
Nov 30, 2024 @ 22:22:20.128	001	win10			CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.	3	19009
Nov 30, 2024 @ 22:20:51.655	001	win10	T1105 T1505	Command and Control, Persistence	[File creation]: Possible web shell scripting file (c:\inetpub\wwwroot\webshell-script.aspx) created	12	100500
Nov 30, 2024 @ 22:20:24.677	001	win10	T1105	Command and Control	Executable file dropped in folder commonly used by malware	15	92213
Nov 30, 2024 @ 22:20:13.281	001	win10	T1053.005	Execution, Persistence, Privilege Escalation	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	92154
Nov 30, 2024 @ 22:20:12.340	001	win10			Software protection service scheduled successfully.	3	60642

ecurity Alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Nov 30, 2024 @ 22:31:02.216	001	win10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Nov 30, 2024 @ 22:31:01.402	001	win10	T1105 T1505	Command and Control, Persistence	[File modification]: Possible web shell content added in c:\inetpub\wwwroot\webshell-script.aspx	12	100501
Nov 30, 2024 @					Windows command prompt started by an abnormal		



2eme Attack :

- **Modification du fichier crée en ajoutant un texte aléatoire 'hello World'**

```
PS C:\Windows\system32> Set-Content -Path 'C:\inetpub\wwwroot\webshell-script.aspx' -Value 'Hello world!'
```

Accéder à l'interface Wazuh pour voir l'alerte :

	16:31:14.578			T1059.003	Execution		
>	Dec 1, 2024 @ 16:31:14.575	001	win10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
>	Dec 1, 2024 @ 16:31:14.250	001	win10	T1105 T1505	Command and Control, Persistence	[File modification]: Possible web shell content added in c:\inetpub\wwwroot\webshell-script.aspx	12	100501

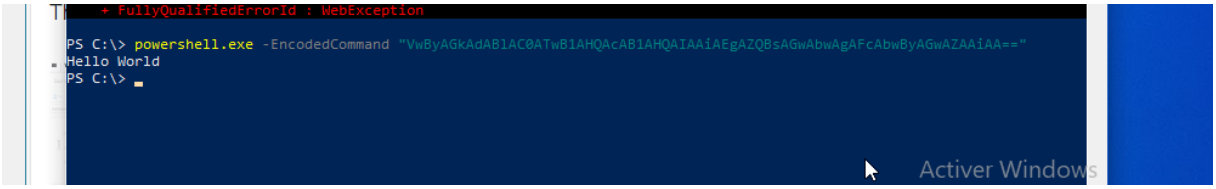
Rows per page: 10 ‹ 1 2 3 ›

Use Case 2 : Emulation d'attaque Power Shell :

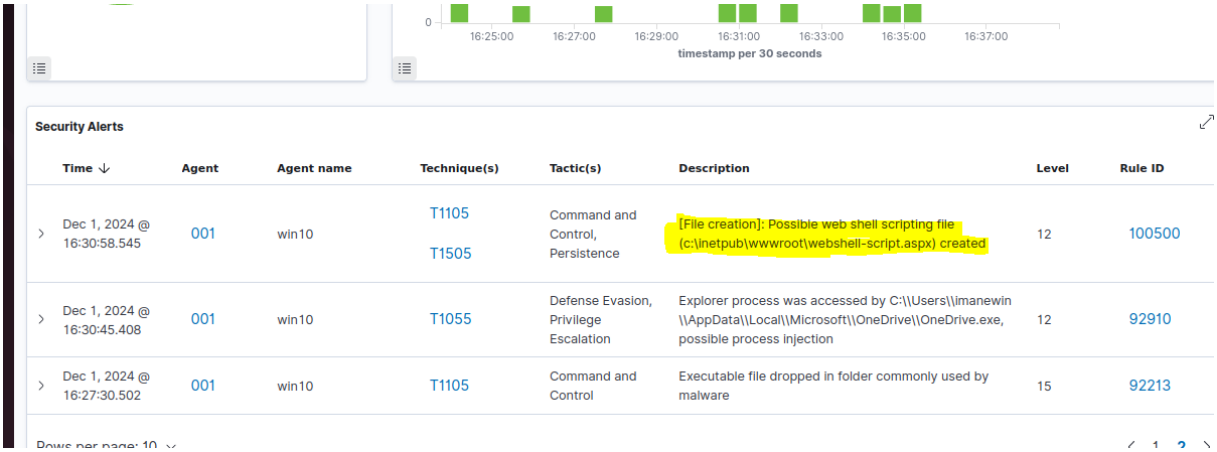
On fait une attaque qui permet de masquer l'intention des scripts et échapper la détection.

(Obfuscation et évasion)

Ouvrir PowerShell en tant qu'Administrateur :



Accéder à l'interface wazuh pour voir l'alerte :



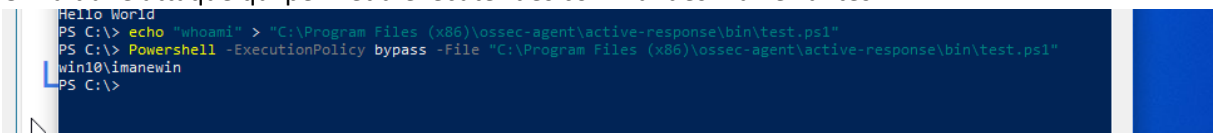
Security Alerts

	Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
>	Dec 1, 2024 @ 16:30:58.545	001	win10	T1105 T1505	Command and Control, Persistence	[File creation]: Possible web shell scripting file (c:\inetpub\wwwroot\webshell-script.aspx) created	12	100500
>	Dec 1, 2024 @ 16:30:45.408	001	win10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\imanewin \\AppData\\Local\\Microsoft\\OneDrive\\OneDrive.exe, possible process injection	12	92910
>	Dec 1, 2024 @ 16:27:30.502	001	win10	T1105	Command and Control	Executable file dropped in folder commonly used by malware	15	92213

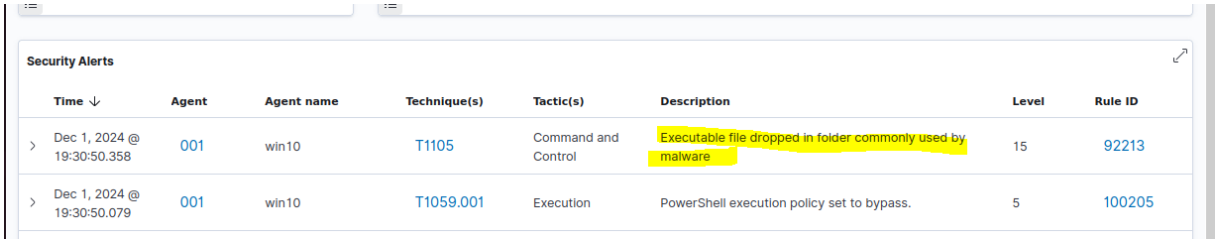
Rows per page: 10 ‹ 1 2 ›

Command and Scripting Interpreter.

On fait une attaque qui permet d'exécuter des commandes malveillantes :



Accéder à l'interface Wazuh pour voir l'alerte :



Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Dec 1, 2024 @ 19:30:50.358	001	win10	T1105	Command and Control	Executable file dropped in folder commonly used by malware	15	92213
Dec 1, 2024 @ 19:30:50.079	001	win10	T1059.001	Execution	PowerShell execution policy set to bypass.	5	100205

Conclusion

Ce mini-projet a permis d'explorer et de mettre en œuvre des cas d'usage de détection basés sur des TTPs issus de l'opération **Soft Cell**, en utilisant le Framework **MITRE ATT&CK**. À travers une approche méthodique, nous avons identifié des techniques spécifiques utilisées par des acteurs malveillants, défini des objectifs de détection clairs et configuré des règles adaptées dans un environnement SOC à l'aide de **Wazuh**.

Les principales réalisations incluent :

- L'identification et le mapping des TTPs avec les IDs **MITRE ATT&CK** appropriés.
- La définition et la configuration de **règles XML** permettant de surveiller et détecter des comportements suspects.
- La validation des règles par des simulations et l'ajustement des paramètres pour réduire les faux positifs.

Ces travaux ont permis d'améliorer la compréhension des mécanismes d'attaque sophistiqués et de renforcer la capacité de détection proactive du SOC. Cependant, il est important de souligner que la cybersécurité est une discipline dynamique. Les attaquants évoluent constamment, ce qui nécessite une mise à jour régulière des règles et des techniques de détection.

Enfin, ce projet met en évidence l'importance d'une approche structurée et basée sur des Framework reconnus comme MITRE ATT&CK pour construire une défense robuste. Les recommandations incluent l'intégration de sources de renseignement sur les menaces (Threat Intelligence) et la formation continue des équipes SOC pour maintenir une posture de sécurité optimisée face à des menaces en constante évolution.