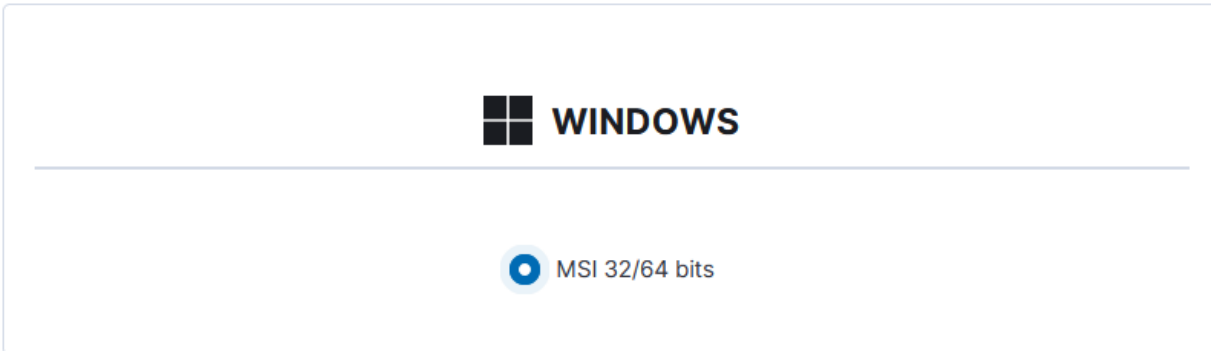
TP WAZUH

TP1- Mise en place de Wazuh et des agents - Thomas Ugo

Tuto : https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html#wazuh-server-node-installation

Installation de l'agent sur un Windows Server

- Déployer un nouvel agent



- Renseignez l'IP de votre serveur :

- Installer l'agent sur le Windows Server avec cette commande powershell : Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.2-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.100.78'

-

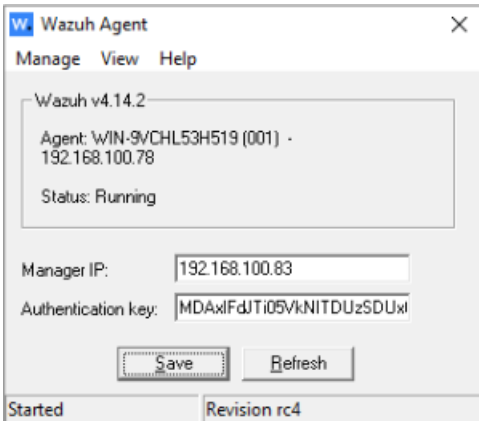
```
PS C:\Users\Administrateur> NET START Wazuh
Le service Wazuh démarre.
Le service Wazuh a démarré.
```

- Ensuite il faudra générer la clé d'authorization.

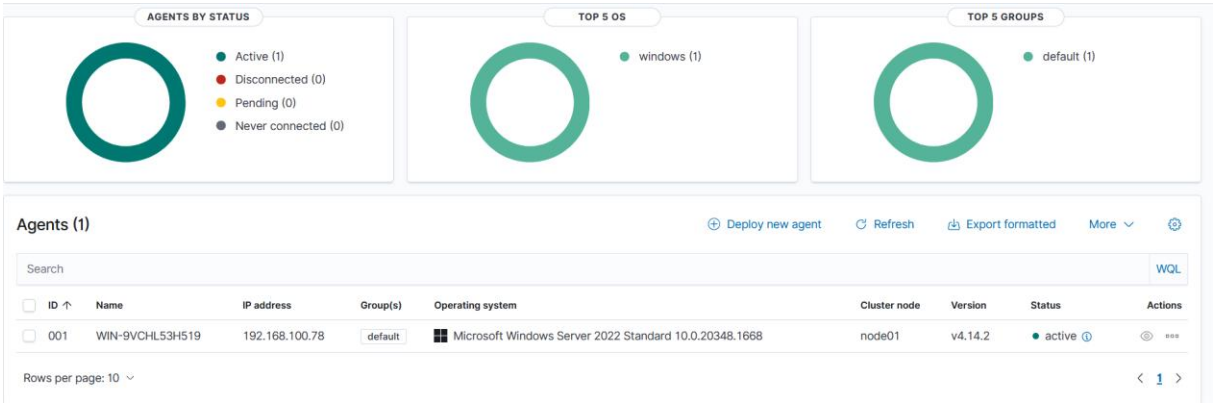
- Aller en mode interactif de Wazuh et renseignez vootre machine

```
root@debian:/home/debian# /var/ossec/bin/manage_agents


****************************************
* Wazuh v4.14.2 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: WIN-9VCHL53H519
   * The IP Address of the new agent: 192.168.100.78
Confirm adding it?(y/n): y
Agent added with ID 001.
```

- Il ne reste plus qu'à extraire la clé de votre machine
- 

- Importer ensuite la clé sur l'agent de votre machine :
- 

- Maintenant sur votre tableau de bord votre machine apparaitra

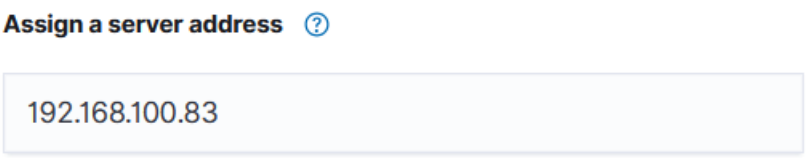


-

Voici le type de logs que l'on peut remonter dans explore --> discover :

Pour un serveur Linux :

- DEB amd64




```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.2-1_amd64.deb && sudo WAZUH_MANAGER='192.168.100.83' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='debian' dpkg -i ./wazuh-agent_4.14.2-1_amd64.deb
```

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Du côté de la machine serveur générer un certificat

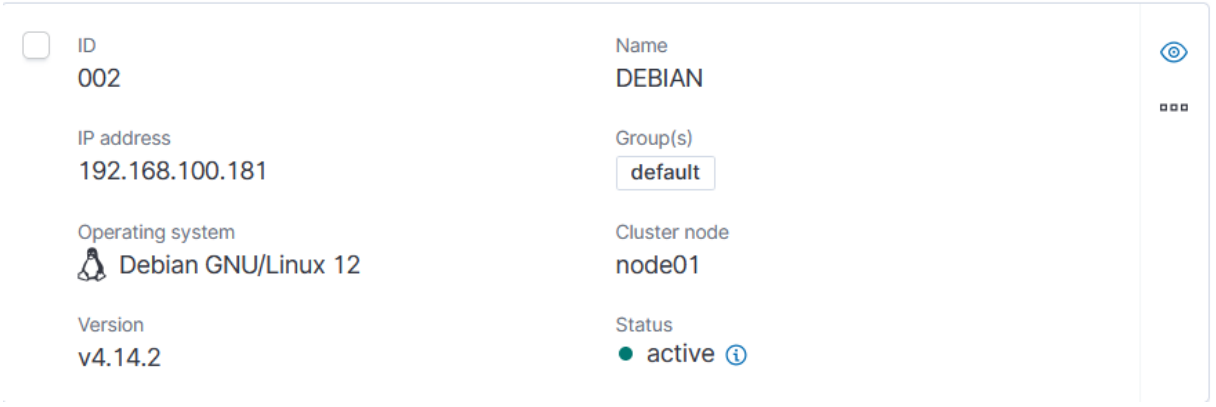
```
root@debian:~# /var/ossec/bin/manage_agents


****************************************
* Wazuh v4.14.2 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: DEBIAN
   * The IP Address of the new agent: 192.168.100.181
Confirm adding it?(y/n): y
Agent added with ID 002.
```

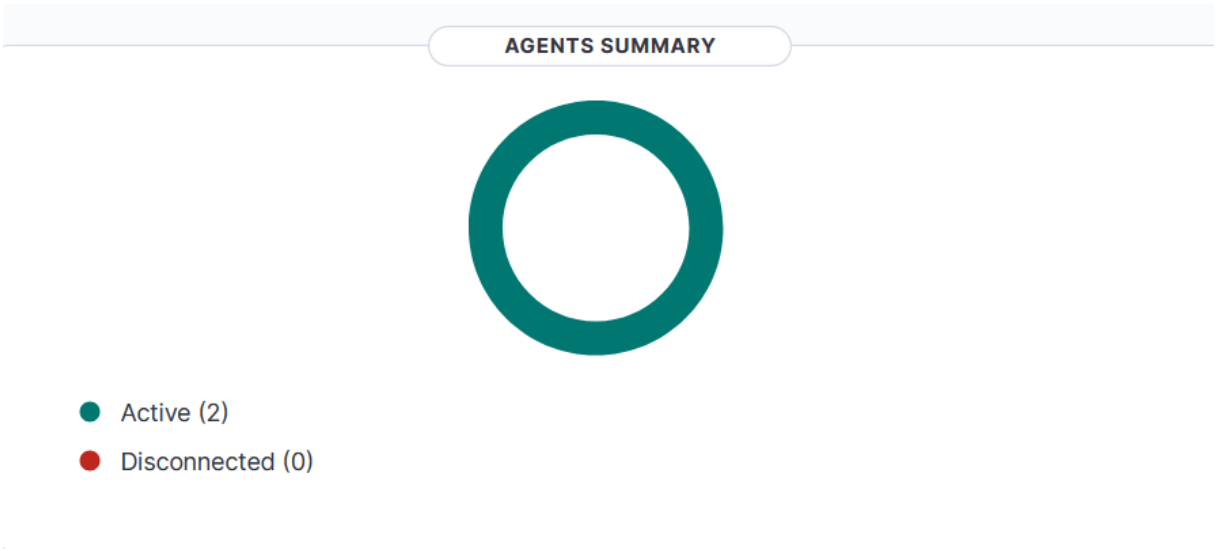
Extraire le certificat :

```
Available agents:
   ID: 001, Name: WIN-9VCHL53H519, IP: 192.168.100.78
   ID: 002, Name: DEBIAN, IP: 192.168.100.181
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIERFQklBTiAxOTIuMTY4LjEwMC4xODEgMjE3Mjk5NDQ4YmUxZWQ2ZTk5NzE0Zjc4Nzg4MWNj
OWRlY2M1OTk4YmI2M2E1Yjc4ZDc3MzU4YzRlZGQ3N2Q5OA==
```

Importer le certificat :

```
****************************************
* Wazuh v4.14.2 Agent manager.         *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAyIERFQklBTiAxOTIuMTY4LjEwMC4xODEgMjE3Mjk
5NDQ4YmUxZWQ2ZTk5NzE0Zjc4Nzg4MWNjOWRlY2M1OTk4YmI2M2E1Yjc4ZDc3MzU4YzRlZGQ3N2Q
5OA==

Agent information:
   ID:002
   Name:DEBIAN
   IP Address:192.168.100.181
```





Voici les logs que l'on remonte :

TP 2 - Attaque par brute force SSH sur serveur Linux (MySQL) UGO

Alerte bruteforce ssh du serveur linux :

Ip source : L'ip source est 192.168.100.102 elle est renseignée dans data.srcip

User ciblé : l'utilisateur ciblé est testuser il est indiqué dans data.srcuser

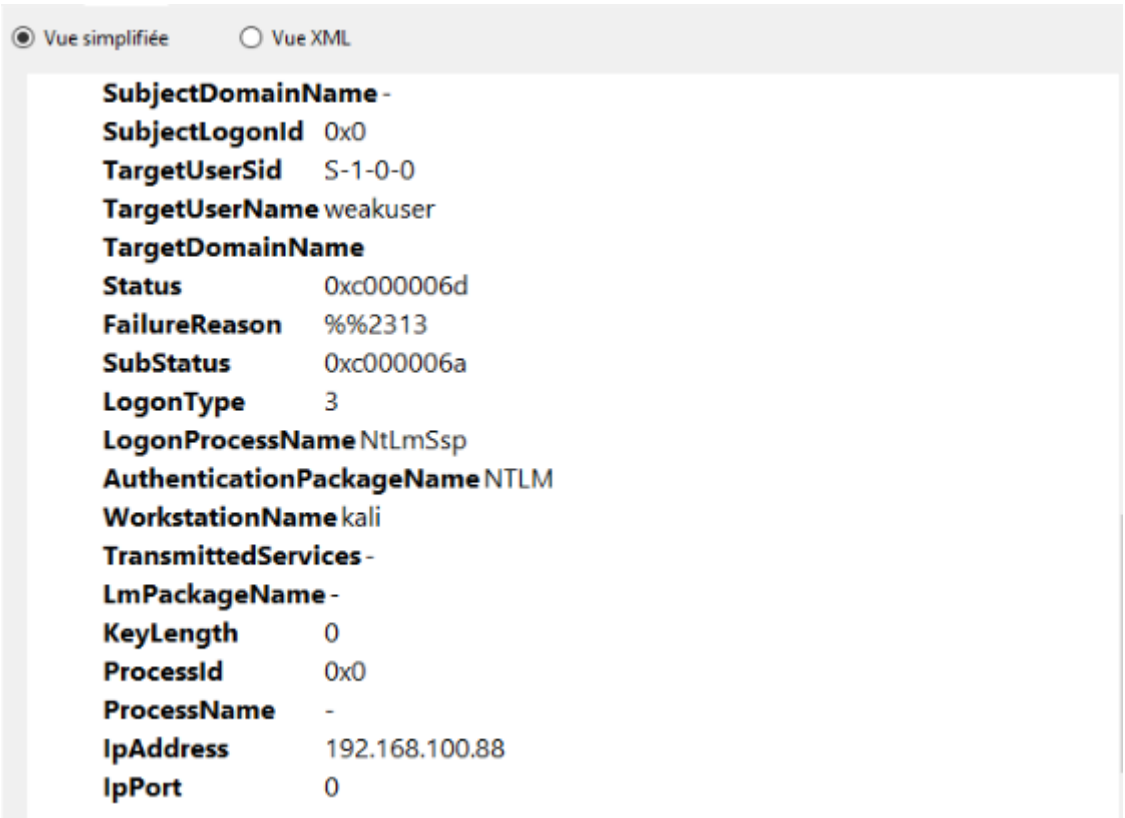
Severité : la sévérité définie par Wazuh est de 5, elle est indiquée dans rule.level

TImeline : `Feb 03 10:50:59 debian sshd[1292]: Invalid user testuser from 192.168.100.102 port 50970`

TP 3 – Vulnérabilités Windows Server – Thomas Ugo

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l weakuser -P /usr/share/wordlists/rockyou.txt -t 4 -s 3389 -f rdp
://192.168.100.78
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-04-07 09:
45:17
[WARNING] the rdp module is experimental. Please test, report - and if possib
le, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p
:14344399), ~3586100 tries per task
[DATA] attacking rdp://192.168.100.78:3389/
[3389][rdp] account on 192.168.100.78 might be valid but account not active f
or remote desktop: login: weakuser password: 123456, continuing attacking the
 account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-04-07 09:
```

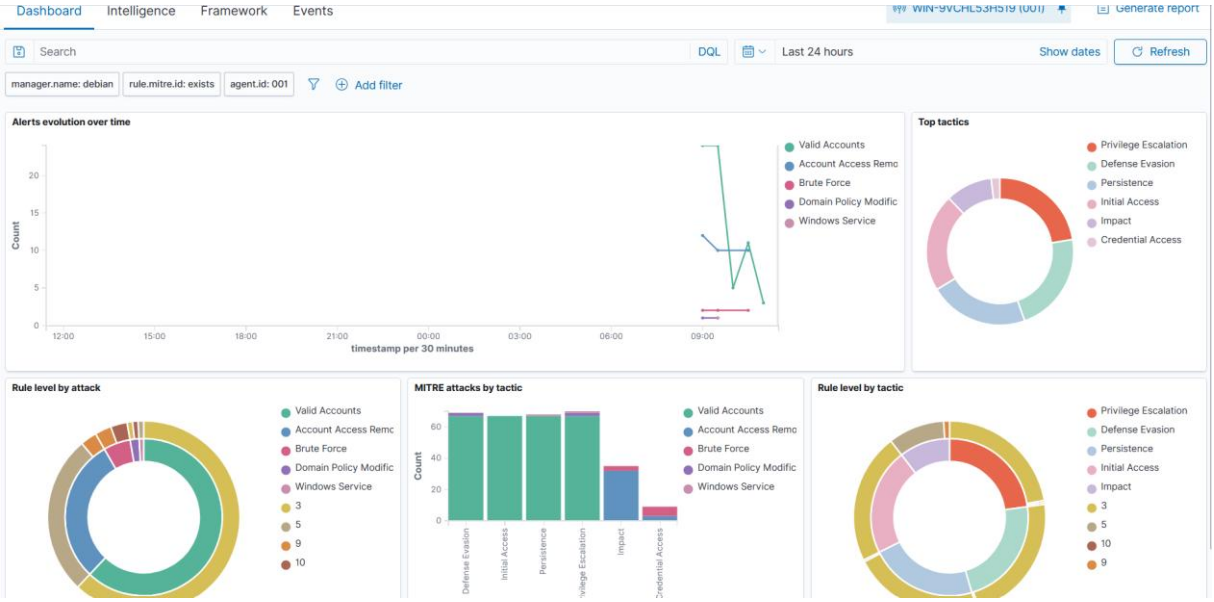
Machine distante :



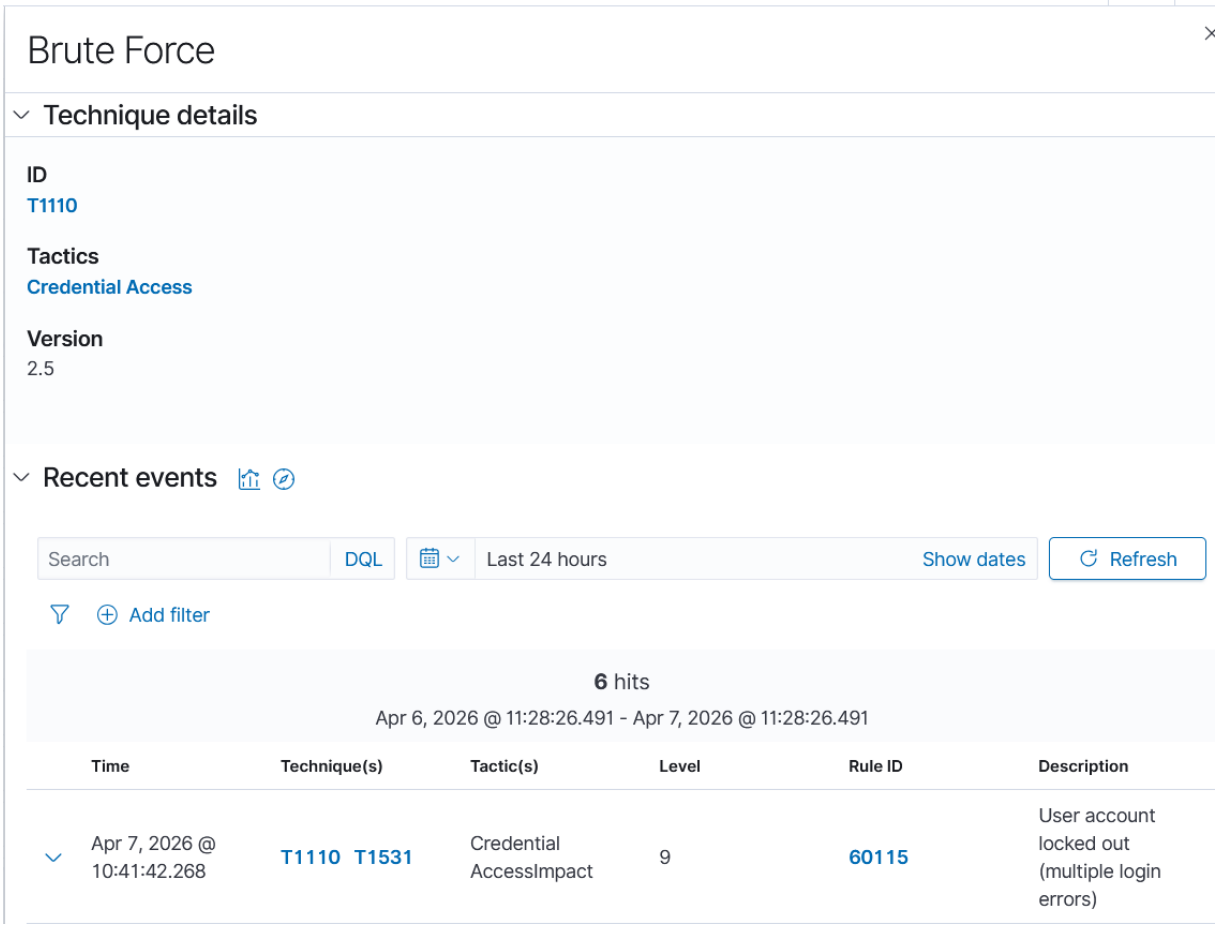
Interprétation des journaux de connexionx :

Le compté ciblé par le brute force est bien le weakuser, la machine qui à attaqué a comme IP source 192.168.100.88 et le nom de cette machine est kali. On voit que la connexion à été refusé mais c'est par raison de sécurité car sur le screen du kali on voit qu'il a bien trouvé le mot de passe . Le Logon type 3 représente une ouverture de session réseau , donc il y a une tentative d'authentification derrière.

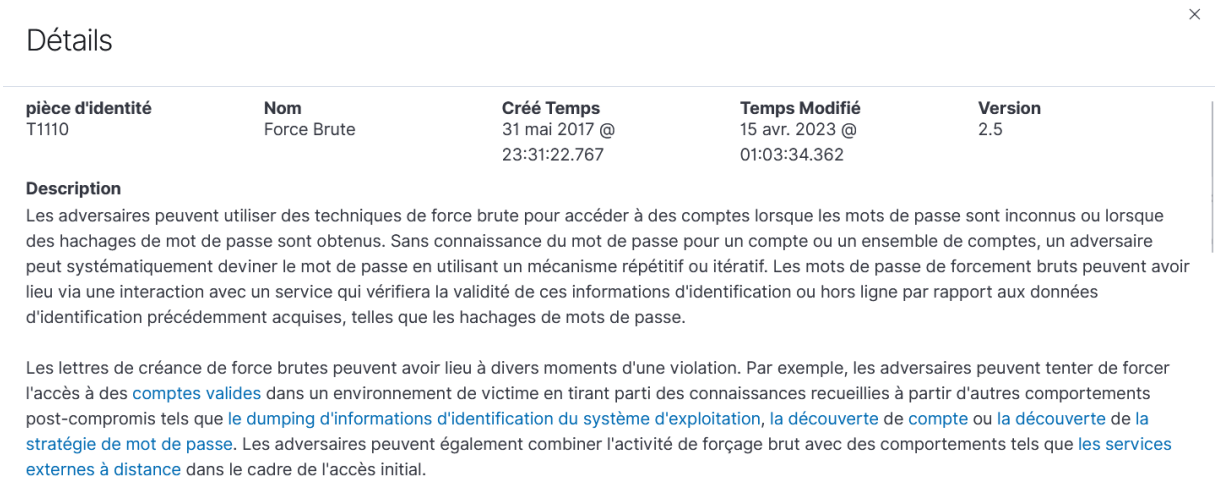
Résumé des statistiques de la machine



Details techniques de l’attaque :



Détail du logs :



Cas 3.2 – Installation d'un service non autorisé (attention aux étapes de manipulation à effectuer en amont sur le serveur Windows

Script que j'ai lancé sur le serveur :

Sans titre1.ps1* Sans titre4.ps1*

```
1  New-Item -ItemType Directory -Path "C:\Temp" -Force
2  Set-Content -Path "C:\Temp\check.ps1" -Value @"
3  while (`$true) {
4      echo "Service actif" >> C:\Temp\service_log.txt
5      Start-Sleep -Seconds 30
6  }
7  "@
```

Sans titre1.ps1* Sans titre4.ps1*

```
1  Get-WinEvent -FilterHashtable @{LogName='System'; Id=7045} | Select-Object TimeCreated, Message | Format-List
2
```

Logs sur le serveur :

Apr 7, 2026 @ 13:43:17.495	WIN-9VCHL53H519	T1543.003	Persistence, Privilege Escalation	New Windows Service Created	5	61138
Apr 7, 2026 @ 13:42:20.195	WIN-9VCHL53H519	T1543.003	Persistence, Privilege Escalation	New Windows Service Created	5	61138

Détail du logs :

Détails

T1543.003	Service Windows	17 janv. 2020 @ 20:13:50.402	21 avr. 2023 @ 14:30:35.872	1.3

Description

Les adversaires peuvent créer ou modifier des services Windows pour exécuter à plusieurs reprises des charges utiles malveillantes dans le cadre de la persistance. Lorsque Windows démarre, il démarre des programmes ou des applications appelés services qui remplissent des fonctions du système d'arrière-plan. Citation: TechNet Services) Les informations de configuration du service Windows, y compris le chemin d'accès aux programmes/commandes exécutables ou de récupération du service, sont stockées dans le registre Windows.

Les adversaires peuvent installer un nouveau service ou modifier un service existant à exécuter au démarrage afin de persister sur un système. Les configurations de service peuvent être définies ou modifiées à l'aide d'utilitaires système (tels que sc.exe), en modifiant directement le Registre ou en interagissant directement avec l'API Windows.

Les adversaires peuvent également utiliser des services pour installer et exécuter des pilotes malveillants. Par exemple, après avoir déposé un fichier de pilote (ex: `.sys`) sur le disque, la charge utile peut être chargée et enregistrée via API native fonctions telles que `CreateServiceW()` (ou manuellement via des fonctions telles que `ZwLoadDriver()` et `ZwSetValueKey()`), en créant les valeurs de service requises (i.e. Modifier le registre), ou en utilisant des utilitaires de ligne de commande tels que `PnPUtil.exe`.(Citation: Symantec W.32 Stuxnet Dossier)(Citation: Crowdstrike DriveSlayer Février 2022) (Citation: Unit42 AcidBox juin 2020) Les adversaires peuvent tirer parti de ces conducteurs comme Rootkitest de cacher la présence d'une activité malveillante sur un système. Les adversaires peuvent également charger un conducteur signé mais vulnérable sur une machine compromise (connue sous le nom de « Bring Your Own Vulnerable Driver » (BYOVD)) dans le cadre de Exploitation pour l'escalade de privilèges.(Citation: ESET InvisiMole Juin 2020)(Citation: Unit42 AcidBox juin 2020)

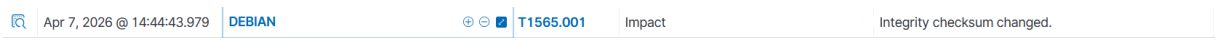
Les services peuvent être créés avec des privilèges d'administrateur, mais sont exécutés sous les privilèges SYSTEM, de sorte qu'un adversaire peut également utiliser un service pour intensifier les privilèges. Les adversaires peuvent également commencer directement les services par l'exécution des services. Pour rendre l'analyse de détection plus difficile, les services malveillants peuvent également intégrer Masquerade Task ou Service (ex: en utilisant un nom de service et / ou de charge utile lié à un OS légitime ou à un composant logiciel bénin).

TP 4 – Vulnérabilités Linux – Thomas Ugo

Cas 4.1 – Modification d'un fichier critique

Modification et ajout de l'utilisateur backdoor sur la machine débian :

Résultat :



Détail du résultat :

pièce d'identité	Nom	Créé Temps	Temps Modifié	Version
T1565.001	Manipulation de données stockées	2 mars 2020 @ 15:22:24.10	Avr 20, 2022 @ 01:03:49.461	1.1

Description

Les adversaires peuvent insérer, supprimer ou manipuler des données au repos afin d'influencer les résultats externes ou de masquer l'activité, menaçant ainsi l'intégrité des données. Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) En manipulant les données stockées, les adversaires peuvent tenter d'affecter un processus d'affaires, une compréhension organisationnelle et une prise de décision.

Les données stockées peuvent inclure une variété de formats de fichiers, tels que des fichiers Office, des bases de données, des e-mails stockés et des formats de fichiers personnalisés. Le type de modification et l'impact qu'elle aura dépend du type de données ainsi que des buts et objectifs de l'adversaire. Pour les systèmes complexes, un adversaire aurait probablement besoin d'une expertise particulière et éventuellement d'un accès à des logiciels spécialisés liés au système qui seraient généralement obtenus grâce à une campagne de collecte d'informations prolongée afin d'avoir l'impact souhaité.

Détails de la technique :

Techniques (750)

Recherche WQL

pièce d'identité	Nom ↑	Description
T1003.008	/etc/passwd et /etc/ombre	Les adversaires peuvent tenter de larguer le contenu de `/etc/passwd` et `/etc/shadow` pour activer le craquage de mot de passe hors ligne. La plupart des systèmes d'exploitation Linux modernes utilisent une combinaison de `/etc/passwd` et `/etc/shadow` pour stocker les informations de compte utilisateur, y compris les hachages de mot de passe dans `/etc/shadow`. Par défaut, `/etc/shadow` est uniquement lisible par l'utilisateur root.(Citation: Mot de passe Linux et formats de fichier d'ombre) L'utilitaire Linux, unshadow, peut être utilisé pour combiner les deux fichiers dans un format adapté aux utilitaires de craquage de mot de passe tels que John the Ripper:(Citation: nixCraft - John the Ripper) `# / usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db`
T1548	Mécanisme de contrôle de l'élévation de l'abus	Les adversaires peuvent contourner les mécanismes conçus pour contrôler les privilèges d'élévation pour obtenir des autorisations de niveau supérieur. La plupart des systèmes modernes contiennent des mécanismes de contrôle d'élévation natifs qui sont destinés à limiter les privilèges qu'un utilisateur peut effectuer sur une machine. L'autorisation doit être accordée à des utilisateurs spécifiques afin d'effectuer des tâches qui peuvent être considérées comme présentant un risque plus élevé. Un adversaire peut effectuer plusieurs méthodes pour tirer parti des mécanismes de contrôle intégrés afin d'intensifier les privilèges sur un système.
		Les adversaires peuvent modifier les jetons d'accès pour fonctionner dans un contexte de sécurité différent de l'utilisateur ou du système pour effectuer des actions et contourner les contrôles d'accès. Windows utilise

Mitre attack

Cas 4.2 – Élévation de privilèges via sudo

Machine débian :

Ajout d’un utilisateur test

```
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_>

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
test ALL=(ALL) NOPASSWD: ALL
```

Détails :

Détails

pièce d'identité	Nom	Créé Temps	Temps Modifié	Version
T1078	Comptes valides	31 mai 2017 @ 23:31:00.645	30 mars 2023 @ 23:01:51.631	2.6

Description

Les adversaires peuvent obtenir et abuser des informations d'identification des comptes existants comme moyen d'obtenir l'accès initial, la persistance, l'escalade de privilège ou l'évasion de défense. Les informations d'identification compromises peuvent être utilisées pour contourner les contrôles d'accès placés sur diverses ressources sur les systèmes du réseau et peuvent même être utilisés pour un accès persistant aux systèmes distants et aux services externes disponibles, tels que les VPN, Outlook Web Access, les périphériques réseau et le bureau à distance. Citation: volexity_0day_sophos_FW) Les informations d'identification compromises peuvent également accorder un privilège accru à un adversaire à des systèmes spécifiques ou à un accès à des zones restreintes du réseau. Les adversaires peuvent choisir de ne pas utiliser de logiciels malveillants ou d'outils en conjonction avec l'accès légitime que ces informations d'identification fournissent pour rendre plus difficile la détection de leur présence.

Dans certains cas, les adversaires peuvent abuser de comptes inactifs: par exemple, ceux qui appartiennent à des personnes qui ne font plus partie d'une organisation. L'utilisation de ces comptes peut permettre à l'adversaire d'échapper à la détection, car l'utilisateur du compte d'origine ne sera pas présent pour identifier toute activité anormale qui a lieu sur son compte.(Citation: CISA MFA PrintNightmare)

Le chevauchement des autorisations pour les comptes locaux, de domaine et de cloud sur un réseau de systèmes est préoccupant car l'adversaire peut être en mesure de pivoter entre les comptes et les systèmes pour atteindre un niveau élevé d'accès (c.-à-d., administrateur de domaine ou d'entreprise) pour contourner les contrôles d'accès définis au sein de l'entreprise. Citation: Vol d'informations d'identification TechNet)

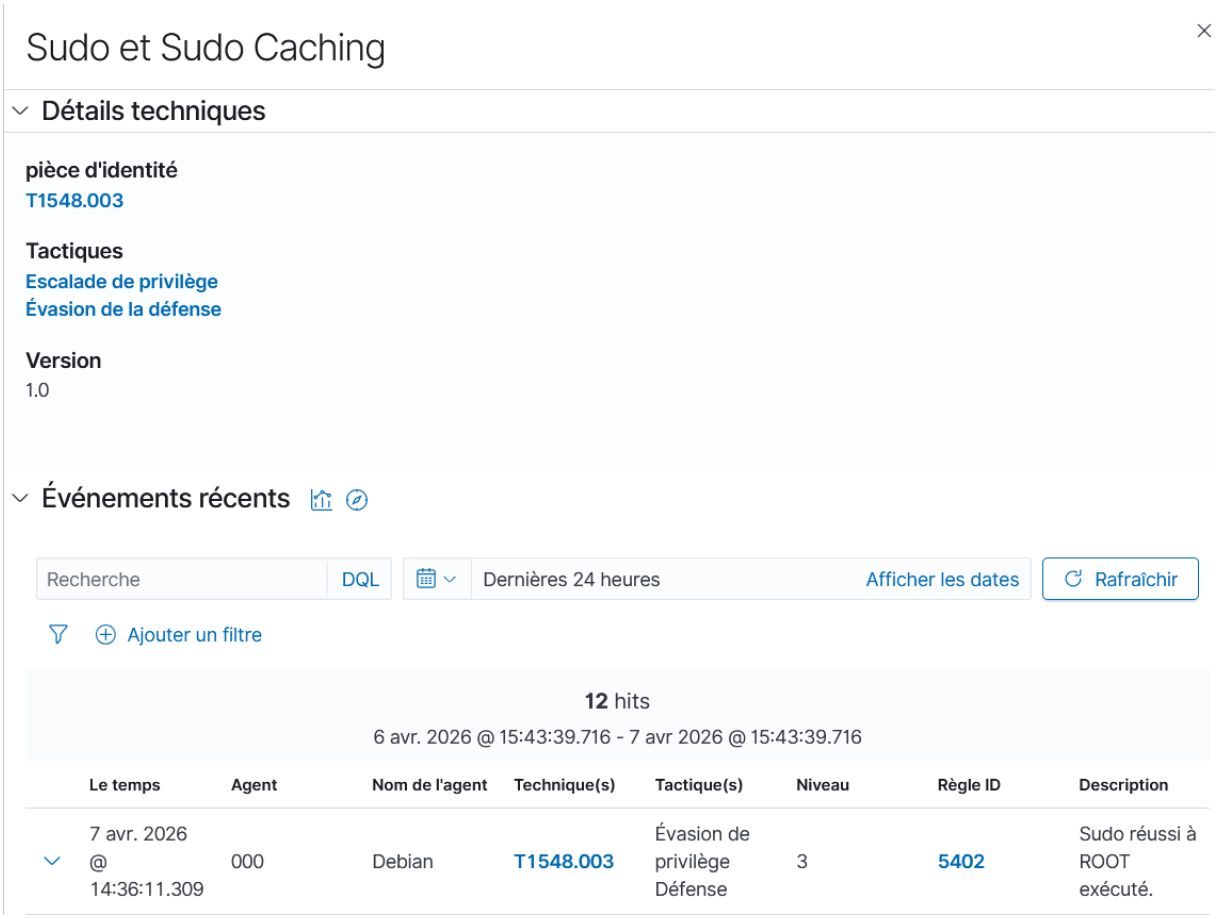
Détails techniques :

Techniques (750)

Recherche WQL

pièce d'identité	Nom ↑	Description
T1003.008	/etc/passwd et /etc/ombre	Les adversaires peuvent tenter de larguer le contenu de `/etc/passwd` et `/etc/shadow` pour activer le craquage de mot de passe hors ligne. La plupart des systèmes d'exploitation Linux modernes utilisent une combinaison de `/etc/passwd` et `/etc/shadow` pour stocker les informations de compte utilisateur, y compris les hachages de mot de passe dans `/etc/shadow`. Par défaut, `/etc/shadow` est uniquement lisible par l'utilisateur root.(Citation: Mot de passe Linux et formats de fichier d'ombre) L'utilitaire Linux, unshadow, peut être utilisé pour combiner les deux fichiers dans un format adapté aux utilitaires de craquage de mot de passe tels que John the Ripper:(Citation: nixCraft - John the Ripper) `# /usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db`
T1548	Mécanisme de contrôle de l'élévation de l'abus	Les adversaires peuvent contourner les mécanismes conçus pour contrôler les privilèges d'élévation pour obtenir des autorisations de niveau supérieur. La plupart des systèmes modernes contiennent des mécanismes de contrôle d'élévation natifs qui sont destinés à limiter les privilèges qu'un utilisateur peut effectuer sur une machine. L'autorisation doit être accordée à des utilisateurs spécifiques afin d'effectuer des tâches qui peuvent être considérées comme présentant un risque plus élevé. Un adversaire peut effectuer plusieurs méthodes pour tirer parti des mécanismes de contrôle intégrés afin d'intensifier les privilèges sur un système.
		Les adversaires peuvent modifier les jetons d'accès pour fonctionner dans un contexte de sécurité différent de l'utilisateur ou du système pour effectuer des actions et contourner les contrôles d'accès. Windows utilise

Mitre Attack :



TP 5 – Synthèse Analyse SOC transversale – Thomas Ugo

Systeme concercné	Type d'incident	Date / heure
Serveur Linux Débian	Brute force ssh	3/02/2026 - 10:50
Windows Server	Brute force sur Windows Server RDP	7/04/2026 - 10h41
Serveur Linux Debian	Manipulation de données stockées	7/04/2026 - 14h46
Serveur Linux Debian	Elevationn de privilèges via sudo	7/04/2026 - 14h36

2) Mapping MITRE ATTACK

	Incident	Systeme	Tactique		Technique	Description	Niveau de risque
INC-01	Brute Force SSH	Linux Debian	TA0006 – Credential Access		T1110 – Brute Force	Tentatives répétées sur le compte `testuser` depuis `192.168.100.102`	CRITIQUE
INC-02	Modification /etc/passwd	Linux Debian	TA0040 – Impact		T1565.001 – Stored Data Manipulation	Manipulation du fichier pour créer un backdoor root	CRITIQUE
INC-03	Dump Credentials	Linux Debian	TA0006 – Credential Access		T1003.008 – `/etc/passwd` et `/etc/shadow`	Extraction des hashes pour craquage offline	CRITIQUE
INC-04	Modification sudoers	Linux Debian	TA0004 – Privilege Escalation		T1548 – Abuse Elevation Control Mechanism	Ajout de `test ALL=(ALL) NOPASSWD: ALL`	CRITIQUE
INC-05	Defense evasion	Linux Debian	TA0005 – Defense Evasion		T1070 – Indicator Removal	Suppression des traces après modification `/etc/passwd`	ELEVEE
INC-06	Brute Fore Windows	Windows Server	TA0006 – Credential Access		T1110 – Brute Force	Tentatives d'accès sur comptes Windows	ELEVEE

4. Reconstituion de la chaine (Fais avec IA pour voir ce qu'il allait proposer)

PHASE 1 — ACCÈS INITIAL

[INC-01] Brute Force SSH (T1110)

→ L'attaquant cible le compte testuser depuis 192.168.100.102

→ Résultat : accès obtenu sur le serveur Linux Debian

↓

PHASE 2 — RECONNAISSANCE INTERNE

[INC-03] Dump /etc/passwd + /etc/shadow (T1003.008)

→ L'attaquant récupère tous les hashes de mots de passe

→ Résultat : credentials de tous les comptes du système

↓

PHASE 3 — ÉLÉVATION DE PRIVILÈGES

[INC-04] Modification sudoers (T1548)

→ Ajout de : test ALL=(ALL) NOPASSWD: ALL

→ Résultat : droits root obtenus sans mot de passe

↓

PHASE 4 — PERSISTANCE

[INC-02] Modification /etc/passwd (T1565.001)

→ Création d'un compte backdoor avec UID 0

→ Résultat : accès root permanent même si le vecteur SSH est coupé

↓

PHASE 5 — DISSIMULATION

[INC-05] Indicator Removal (T1070)

→ Suppression du backdoor dans /etc/passwd, effacement historique

→ Résultat : traces effacées, compromission difficile à détecter

↓

PHASE 6 — MOUVEMENT LATÉRAL

[INC-06] Brute Force Windows Server (T1110)

→ Utilisation des credentials récupérés via /etc/shadow

→ Résultat : tentative de propagation vers Windows Server

Priorité	Incident	Technique	Niveau	Justification
P1	Brute Force SSH (INC-01)		CRITIQUE	Point d'entrée de toute la chaîne
P2	Modification sudoers (INC-04)		CRITIQUE	Donne les droits root à l'attaquant
P3	Modification `/etc/passwd` (INC-02)		CRITIQUE	Persistance root permanente
P4	Dump credentials (INC-03)		CRITIQUE	Expose tous les mots de passe
P5	Indicator Removal (INC-05)			Efface les preuves
P6	Brute Force Windows (INC-06)			Mouvement latéral en cours