LIVRABLE DE PROJET

10/12/2024 - SAE 5.CYBER 3 - ASSURER LA SÉCURISATION ET LA SUPERVISION AVANCÉE D'UN SYSTÈME D'INFORMATION

—— ORION TEAM

MAHADALI Neil

DITTOO Farhan

DUFOSSE Jacob

PIGNOLET Matthieu

Sommaire

1. Introduction et contexte

A. Contexte du Projet

Dans un contexte professionnel où les cybermenaces sont de plus en plus fréquentes et sophistiquées, la sécurisation et la supervision avancée des systèmes d'information deviennent des enjeux stratégiques pour les entreprises. Le projet SAE 5.CYBER 3 a été conçu pour répondre à ces défis en mettant en place une infrastructure sécurisée et segmentée, intégrant des solutions avancées de supervision, de gestion des identités et de détection des menaces.

B. Objectifs du Projet

L'objectif principal de ce projet est d'assurer la protection des actifs numériques d'une entreprise en déployant un SOC (Security Operations Center) léger et efficace, capable de superviser et de sécuriser l'ensemble des systèmes critiques. Cette infrastructure doit permettre :

- Une centralisation de la supervision et une gestion optimisée des incidents de sécurité.
- Une segmentation stricte du réseau afin de minimiser les risques de compromission.
- Une gestion avancée des flux réseau pour garantir la disponibilité des services essentiels.

C. Solutions Déployées

Pour répondre à ces besoins, nous avons mis en place une architecture robuste intégrant les composants suivants :

Pare-feu OPNsense

- Configuration avancée des règles de filtrage pour sécuriser les flux entrants et sortants.
- Activation des modules IDS/IPS (Intrusion Detection/Prevention Systems) pour bloquer les activités malveillantes.
- Intégration avec CrowdSec pour une détection proactive des menaces.

SOC (Security Operations Center)

- **Wazuh (SIEM)** : Collecte et corrélation des logs pour une détection avancée des intrusions.
- **Zabbix** : Supervision des performances des systèmes et surveillance réseau en temps réel.
- **Grafana** : Visualisation et analyse des métriques de sécurité.
- **Deming** : Gestion et reporting de la conformité aux normes de cybersécurité.
- **Mercator** : Cartographie des systèmes d'information pour une meilleure visibilité et gouvernance.

Infrastructure de Gestion des Identités

- **Active Directory** : Administration centralisée des utilisateurs et des ressources.
- **Politiques GPO (Group Policy Objects)** : Renforcement des stratégies de sécurité.
- **Durcissement d'AD (Harden AD)** : Application des meilleures pratiques pour sécuriser l'annuaire Active Directory.

Bastion Sécurisé avec Teleport

- Accès restreint et authentification multi-facteurs (MFA) pour les administrateurs.
- Journalisation complète des connexions pour assurer la traçabilité des actions.
- Proxy unique permettant une gestion fine des accès aux ressources critiques.

Zone Front et Services Exposés

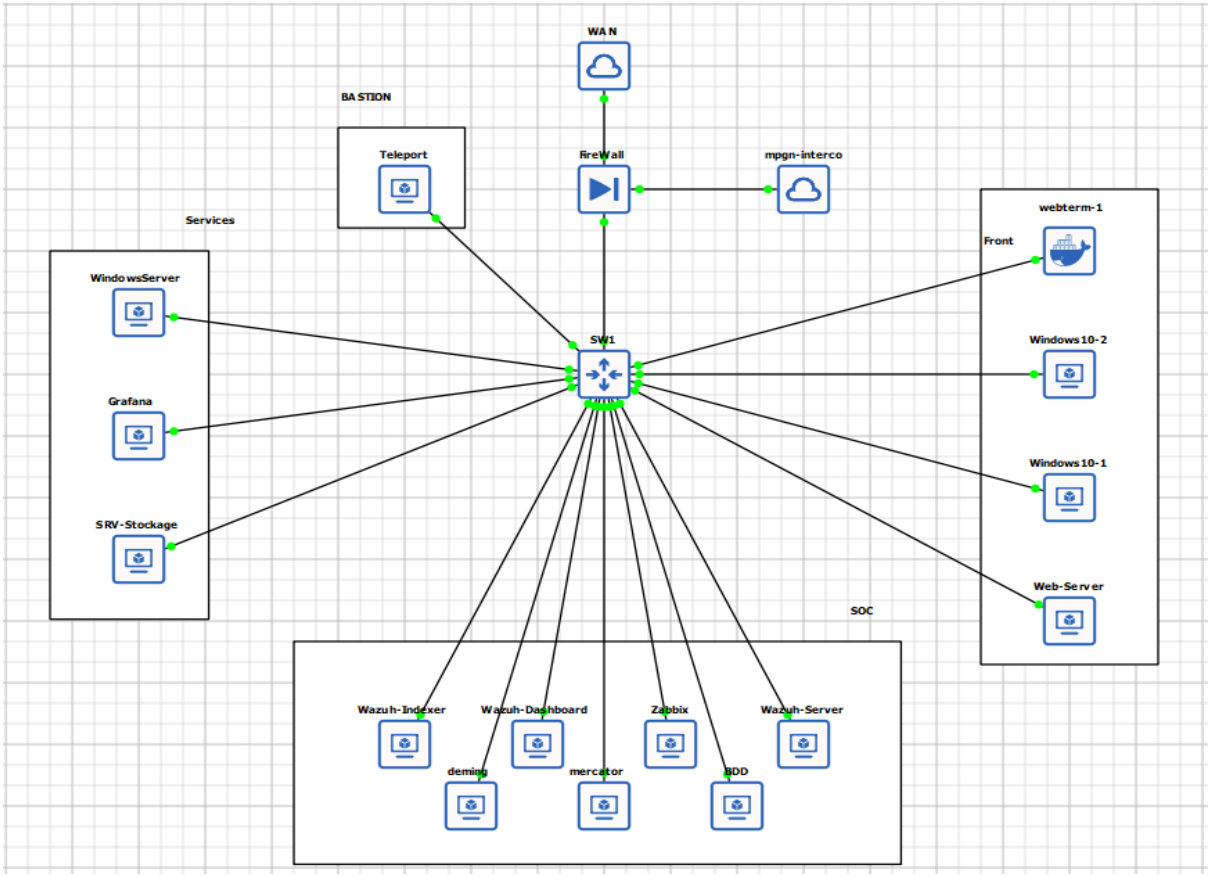
- **Webserver sécurisé** : Protection des applications web avec un proxy inversé et un WAF (Web Application Firewall).
- **Isolation des services internes** pour limiter les risques d'exposition aux attaques externes.

Audit de Sécurité et Résultats

Afin d'évaluer l'efficacité de l'infrastructure mise en place, un audit de sécurité a été réalisé, incluant :

- **Audit PingCastle** : Évaluation des vulnérabilités Active Directory avant et après le durcissement.
- **Pentest d'un site WordPress** : Détection et exploitation de vulnérabilités critiques (CVE-2008-1930).
- **Validation des mesures de remédiation** : Test des mécanismes de protection (pare-feu, Wazuh, CrowdSec, GPO).

2. Détails de la topologie réseau



La topologie est segmentée en plusieurs zones, avec un **pare-feu central** comme point de contrôle du trafic.

Voici une description détaillée de chaque composant :

2.1. Pare-feu (OPNSENSE)

A. Fonction

Le pare-feu OPNsense est utilisé pour le contrôle et le filtrage du trafic réseau entre les différentes zones du réseau. Il assure la sécurité et la segmentation des communications.

Configuration

Interface WAN :

- Connectée à l'extérieur via une adresse IP publique.
- Gère l'accès aux ressources externes et redirige les flux autorisés vers le réseau interne.

Interface INTERCO :

- Permet un accès global aux équipements pour la configuration et l'administration de toute la topologie réseau.
- Facilite la gestion centralisée des différentes zones et services.

Interface LAN :

- Connectée aux VLANs internes.
- Permet la segmentation des réseaux internes pour une meilleure sécurité et organisation.

Interface ADMIN :

- Assignée pour le réseau administratif, entièrement séparé des autres VLANs.
- Configuration de l'adresse réseau **10.81.255.1/24**.
- Assure une isolation stricte pour la gestion des équipements administratifs.

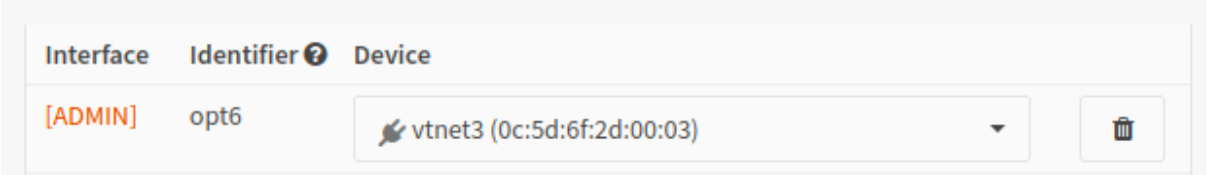
Règles de pare-feu mises en place

Source	Destination	Protocole	Port(s)	Description
BASTION, FRONT, SERVICE, SOC	Active Directory	TCP/UDP	389 (LDAP), 53 (DNS), 445 (MS DS), 135, 636, 88	Ports nécessaires pour l'active directory
BASTION, FRONT, SERVICE, SOC	BASTION	TCP	443	Connexion des hôtes pour les agents Teleport
BASTION, FRONT, SERVICE, SOC	Wazuh-Manager	TCP	1515	Accès des agents Wazuh au Wazuh Manager
BASTION, FRONT, SERVICE, SOC	Wazuh-Manager	TCP	1514	Accès des agents Wazuh au Wazuh Manager.
BASTION, FRONT, SERVICE, SOC	Wazuh-Manager	TCP	55000	Accès à l'api RESTful de Wazuh
BASTION, FRONT, SERVICE, SOC	Zabbix	TCP/UDP	10051	Accès vers le collecteur Zabbix pour les agents
BASTION, FRONT, SERVICE, SOC	Firewall	TCP	8080	Utilisé par CrowdSec
ADMIN	any	any	any	Accès du réseau admin à tout
BASTION	FRONT, SERVICE, SOC	TCP	22 (SSH), 80 (HTTP), 443 (HTTPS)	Autoriser le bastion à se connecter
SERVICE	10.81.110.110 (Zabbix)	TCP	80 (HTTP)	Connexion de Grafana à l'api Zabbix
SOC	10.81.255.1/24 10.81.140.1/24 10.81.130.1/24 10.81.150.1/24 10.81.120.1/24 10.81.110.1/24	TCP/UDP	10050	Connexion de Zabbix à ses agents pour le polling

1. Réseau ADMIN

Nous avons assigner une interface pour le réseau admin qui sera séparé entièrement des autres VLAN

Assigner une nouvelle interface pour le réseau admin qui sera entièrement séparé



2.2. Zone SOC (10.81.110.0/24)

Description générale :

La zone SOC est dédiée à l'hébergement des outils de **supervision** et de **détection des menaces**, offrant une plateforme centralisée pour assurer la sécurité, la performance et la résilience des systèmes d'information.

Composants hébergés :

1. **Wazuh :**
   - **Wazuh Manager** : Gère la corrélation des événements et la supervision des agents.
   - **Wazuh Dashboard** : Interface utilisateur pour la visualisation des événements de sécurité.
   - **Wazuh Indexer** : Indexe et stocke les journaux pour faciliter leur recherche et analyse.
2. **CrowdSec :**
   - Fournit une **protection collaborative** contre les menaces réseau en identifiant et bloquant les comportements malveillants.
3. **Zabbix :**
   - Plateforme de **supervision réseau** et d'infrastructure pour surveiller les performances et la disponibilité.
4. **BDD (Base de Données Zabbix)** :
   - Base de données dédiée à Zabbix pour le stockage des métriques et des journaux collectés.

5. **Deming :**
    - **Outil ISO/IEC 27001:2013 (chapitre 9)** pour la gestion, la planification, la surveillance et le reporting de l'efficacité des mesures de sécurité.
    - **Principales fonctionnalités :**
        - Évaluer l'efficacité des contrôles en place.
        - Vérifier les exigences de sécurité.
        - Améliorer continuellement le système de gestion de la sécurité de l'information (ISMS).
        - Analyse et reporting pour une prise de décision basée sur des données fiables.
6. **Mercator :**
    - Application web open-source pour la **cartographie des systèmes d'information**, conforme au **Guide de la cartographie des systèmes d'information** de l'ANSSI.
    - **Objectifs principaux :**
        - Faciliter la visibilité et la gestion des systèmes d'information.
        - Renforcer le contrôle et la résilience des infrastructures critiques.
        - Soutenir la gouvernance IT pour une meilleure gestion des actifs.

Connectivité et flux réseau :

- **Accès restreint aux administrateurs :**
  L'accès aux machines virtuelles de la zone SOC est limité via un bastion sécurisé.
- **Flux de journaux centralisés :**
  Collecte et centralisation des journaux provenant des autres zones pour leur traitement et leur analyse dans le SOC.

Liste des machines virtuelles dans la zone SOC :

1. **Wazuh-Indexer** : Assure l'indexation des journaux pour les recherches et analyses.
2. **Wazuh-Dashboard** : Interface de visualisation et de gestion des événements.
3. **Wazuh-Manager** : Gère les agents et applique les règles de sécurité.
4. **CrowdSec** : Protection collaborative contre les menaces.
5. **Zabbix** : Plateforme principale de supervision.
6. **BDD** : Base de données Zabbix pour le stockage des métriques.
7. **Deming** : Évaluation, gestion et amélioration des mesures de sécurité.
8. **Mercator** : Cartographie des systèmes d'information pour une meilleure visibilité et gouvernance.

2.3. Zone Services (10.81.120.0/24)

- Conçue pour héberger des services internes critiques :
  - **Grafana** : Visualisation des données réseau et système rassemblant les données de wazuh et zabbix.
  - **SRV-Stockage** : Serveur de stockage pour les données critiques.
  - **WindowsServer** : Active Directory (AD) pour la gestion des identités et des accès.
- Connectivité :
  - Flux restreints aux communications internes avec le SOC.
  - Accès direct depuis l'extérieur interdit.

2.4. Zone Front (10.81.130.0/24)

Description générale :

La zone **Front** expose les services publics de l'entreprise, tels que les applications web, tout en sécurisant les connexions entrantes grâce à un proxy inversé.

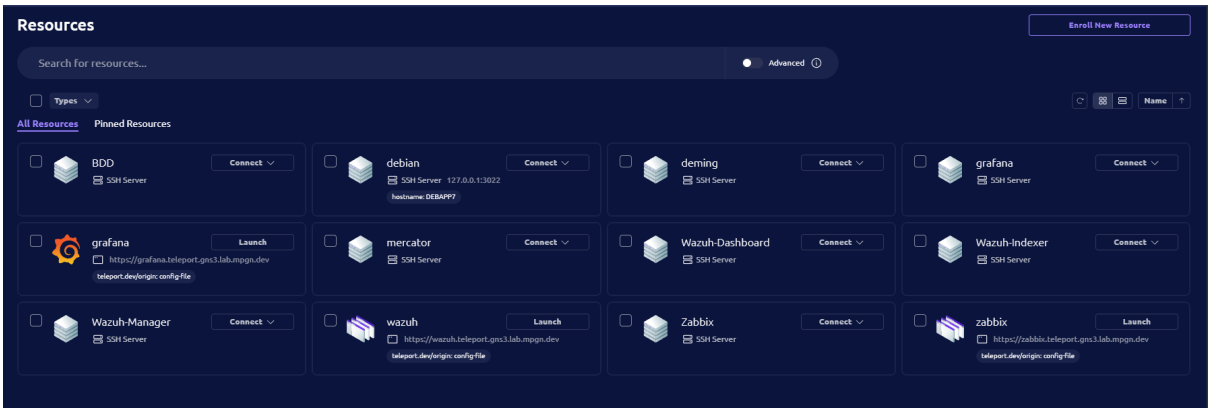
Composants hébergés :

1. **webterm-1 (conteneur Docker) :**
    - Permet l'hébergement d'applications web accessibles depuis l'extérieur.
2. **Windows10-1 :**
    - Poste de travail utilisé pour des tests ou des interactions spécifiques dans la zone.
3. **Windows10-2 :**
    - Poste de travail utilisé pour des tests ou des interactions spécifiques dans la zone.
4. **webserver-1 :**
    - Héberge un environnement WordPress dédié aux tests d'audit de sécurité.

Connectivité et sécurisation :

- **Isolation des services internes** :
    - Les services internes critiques (comme Active Directory ou d'autres ressources internes) ne sont **pas accessibles** depuis la zone Front sauf pour les clients Windows

2.5. Bastion (Teleport)



Fonction : Point d'entrée unique et sécurisé pour les connexions administratives.

Configuration :

- Accès exclusif via un VPN sécurisé.
- Journalisation détaillée des connexions à des fins d'audit et de traçabilité.

Accès autorisés :

- Interfaces Web :
  - Grafana
  - Wazuh-Dashboard
  - Zabbix

- Connexions SSH directes aux serveurs suivants :
    - BDD
    - Teleport
    - Deming
    - Grafana
    - Mercator
    - Wazuh-Dashboard
    - Wazuh-Indexer
    - Wazuh-Manager
    - Zabbix

Ce serveur bastion centralise et sécurise l'accès aux ressources critiques, garantissant une gestion administrative contrôlée et traçable.

2.6. Connectivité entre les zones

- **VLAN distincts** pour chaque zone.
- **Routage configuré sur le pare-feu** avec des règles spécifiques pour limiter le trafic.
- **Inspection approfondie des paquets** pour détecter les anomalies.

3. Configuration des serveurs

3.1. Serveurs SOC

A. Wazuh

Dans la zone SOC, les composants de **Wazuh** ont été séparés sur trois serveurs distincts afin d'assurer une meilleure performance, une scalabilité optimisée et une gestion simplifiée des ressources.

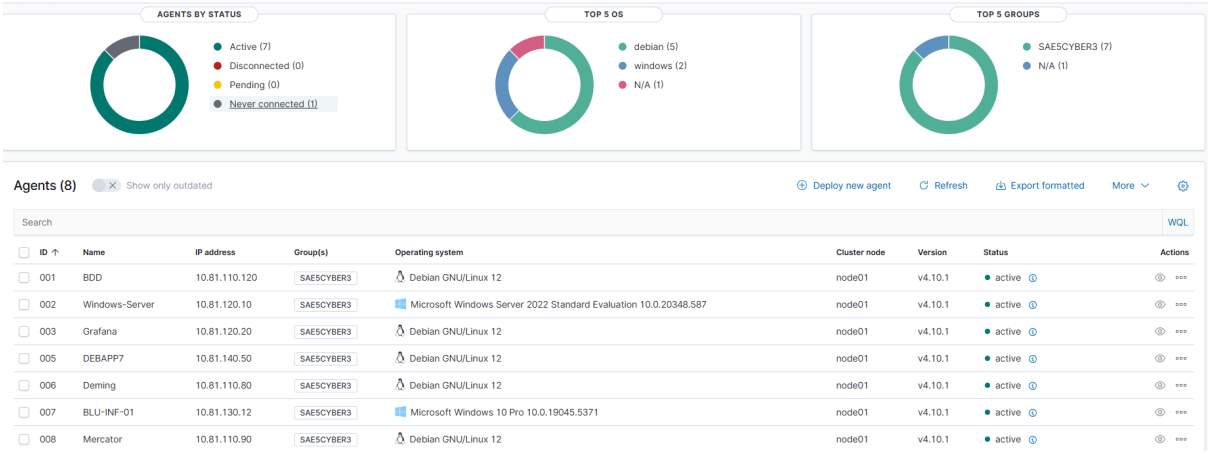
Détails des serveurs :

1. **Wazuh-Indexer**
    - **Adresse IP** : `10.81.110.60`
    - **Rôle** : Assure l'indexation et le stockage des journaux pour permettre des recherches rapides et efficaces.
2. **Wazuh-Dashboard**
    - **Adresse IP** : `10.81.110.50`
    - **Rôle** : Fournit une interface graphique intuitive pour la visualisation et la gestion des événements de sécurité.
3. **Wazuh-Manager**
    - **Adresse IP** : `10.81.110.70`
    - **Rôle** : Coordonne la gestion des agents, applique les règles de corrélation et centralise les données de sécurité.

Avantages de la séparation des composants :

- **Performance accrue** : Chaque composant est exécuté sur un serveur dédié, réduisant la charge et les conflits entre les services.
- **Scalabilité** : La séparation permet d'ajouter ou de modifier les composants sans perturber les autres services.
- **Gestion simplifiée** : Une meilleure isolation des rôles facilite la maintenance et le diagnostic en cas de problème.

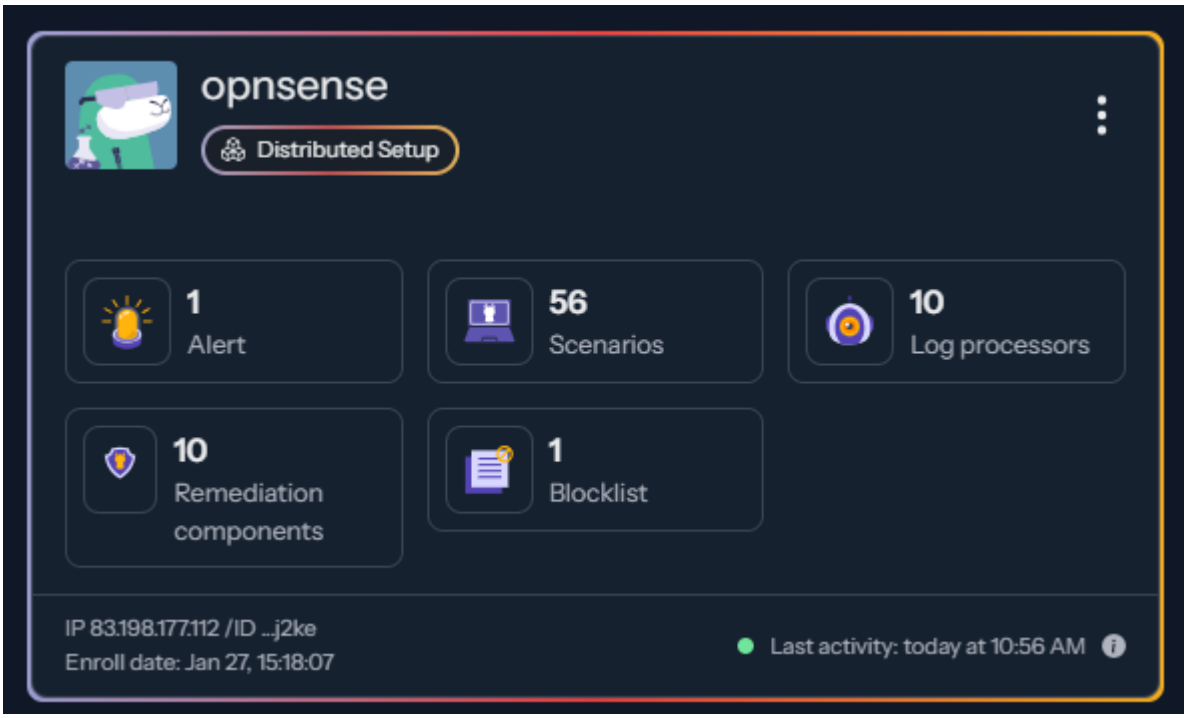
Monitoring des agents :



Voici une liste résumée des agents :

1. **BDD** - 10.81.110.120 - Debian GNU/Linux 12
2. **Windows-Server** - 10.81.120.10 - Windows Server 2022
3. **Grafana** - 10.81.120.20 - Debian GNU/Linux 12
4. **DEBAPP7** - 10.81.140.50 - Debian GNU/Linux 12
5. **Deming** - 10.81.110.80 - Debian GNU/Linux 12
6. **BLU-INF-01** - 10.81.130.12 - Windows 10 Pro
7. **Mercator** - 10.81.110.90 - Debian GNU/Linux 1

B. Crowdsec



Fonctionnalités principales :

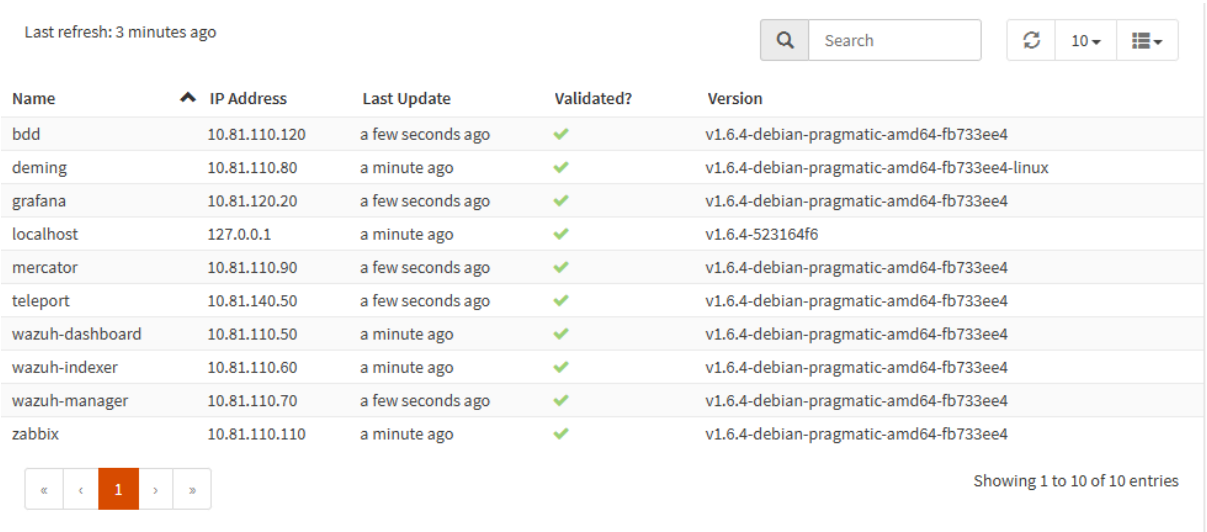
1. Déploiement en mode serveur :

- **Détection d'attaques sur l'ensemble du réseau :**
  CrowdSec est capable d'analyser les flux réseau pour identifier les comportements malveillants (tentatives de brute-force, scans de ports, etc.) et détecter les menaces en temps réel.
- **Centralisation des informations collectées :**
  Les données collectées sur les menaces et comportements suspects sont centralisées, facilitant l'analyse et la prise de décision.

2. Intégration avec OPNsense :

- **Automatisation des blocages d'IP malveillantes :**
  Grâce au **plugin CrowdSec** installé sur OPNsense, les décisions de blocage d'IP malveillantes sont appliquées automatiquement, renforçant la sécurité du pare-feu.
- **Synchronisation avec les règles du pare-feu :**
  Les décisions prises par CrowdSec (via la base de données collaborative de menaces et les analyses locales) sont synchronisées avec les règles d'OPNsense, offrant une protection active et dynamique contre les menaces.
- **Protection collaborative :**
  L'intégration permet de bénéficier d'une base de données partagée des menaces, enrichie par d'autres utilisateurs de CrowdSec, pour anticiper et bloquer de nouvelles attaques.

3. Configuration de l'agent sur OPNsense :



Last refresh: 3 minutes ago

Search 10

Name	IP Address	Last Update	Validated?	Version
bdd	10.81.110.120	a few seconds ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4
deming	10.81.110.80	a minute ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4-linux
grafana	10.81.120.20	a few seconds ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4
localhost	127.0.0.1	a minute ago	✔	v1.6.4-523164f6
mercator	10.81.110.90	a few seconds ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4
teleport	10.81.140.50	a few seconds ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4
wazuh-dashboard	10.81.110.50	a minute ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4
wazuh-indexer	10.81.110.60	a minute ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4
wazuh-manager	10.81.110.70	a few seconds ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4
zabbix	10.81.110.110	a minute ago	✔	v1.6.4-debian-pragmatic-amd64-fb733ee4

« ‹ 1 › »

Showing 1 to 10 of 10 entries

Agent CrowdSec installé :

- **Sur chaque serveur** (Wazuh-Indexer, Wazuh-Dashboard, Wazuh-Manager, Zabbix, etc.), un **agent CrowdSec** est installé pour surveiller les événements spécifiques à ce serveur.
- Cet agent analyse les journaux locaux (logs système, tentatives d'accès, etc.) pour détecter des comportements malveillants en temps réel.
- Cela permet une détection granulaire des menaces, directement à la source des événements.

Connexion à LAPI (Local API) d'OPNsense :

- Tous les agents CrowdSec déployés sur les serveurs de la zone SOC sont connectés à l'**API locale (LAPI)** de CrowdSec, hébergée sur OPNsense.
- Cette connexion centralise les informations collectées par les agents sur chaque serveur et transmet les décisions (blocages, alertes) au pare-feu OPNsense.
- En cas de détection d'une IP malveillante par l'un des agents, la LAPI d'OPNsense applique rapidement les règles nécessaires pour bloquer cette IP à l'échelle du réseau.

Avantages de cette architecture :

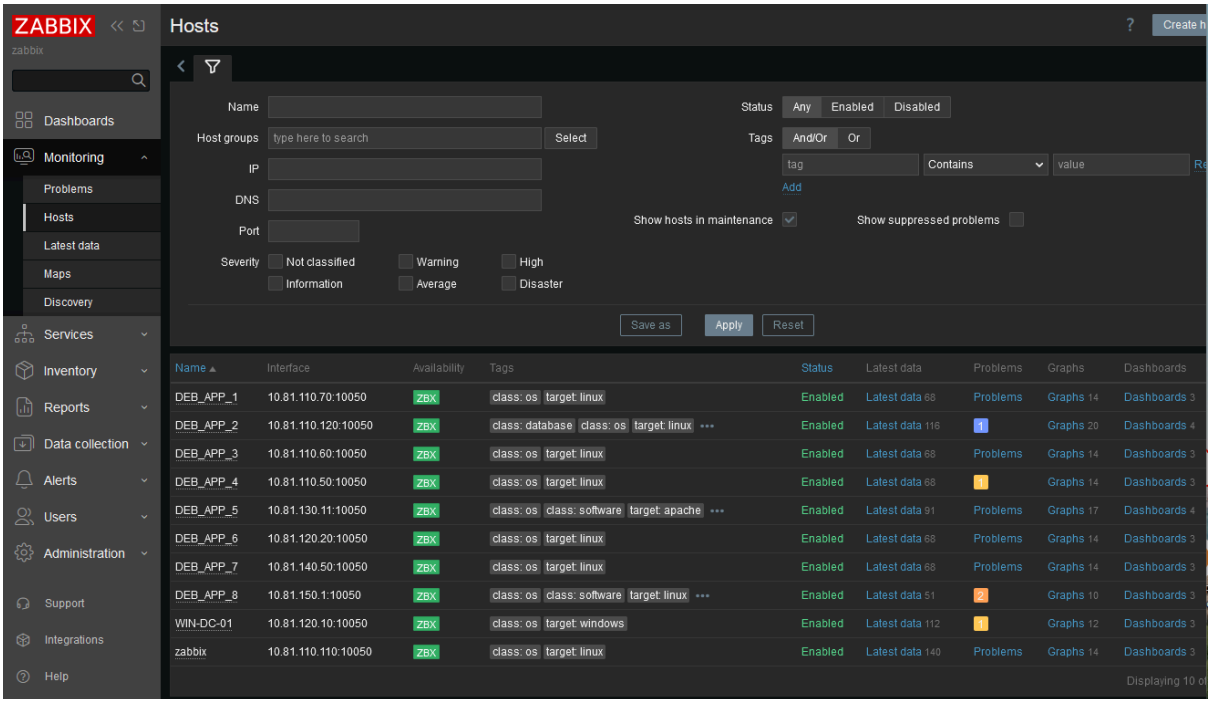
1. **Protection distribuée et synchronisée :**
    - Chaque serveur agit comme un point de détection pour les menaces qui lui sont propres.
    - Les décisions prises par les agents sont synchronisées avec OPNsense, permettant une réponse globale et coordonnée.
2. **Réaction rapide :**
    - La connexion entre les agents et LAPI garantit que les blocages d'IP malveillantes sont appliqués quasi instantanément à travers le pare-feu.
3. **Centralisation des décisions :**
    - Les agents installés sur chaque serveur renforcent la visibilité globale des menaces, tout en déchargeant les ressources d'OPNsense en répartissant les analyses.

C. Architecture et Configuration Zabbix

1. Architecture système

L'infrastructure de supervision repose sur une architecture distribuée avec :

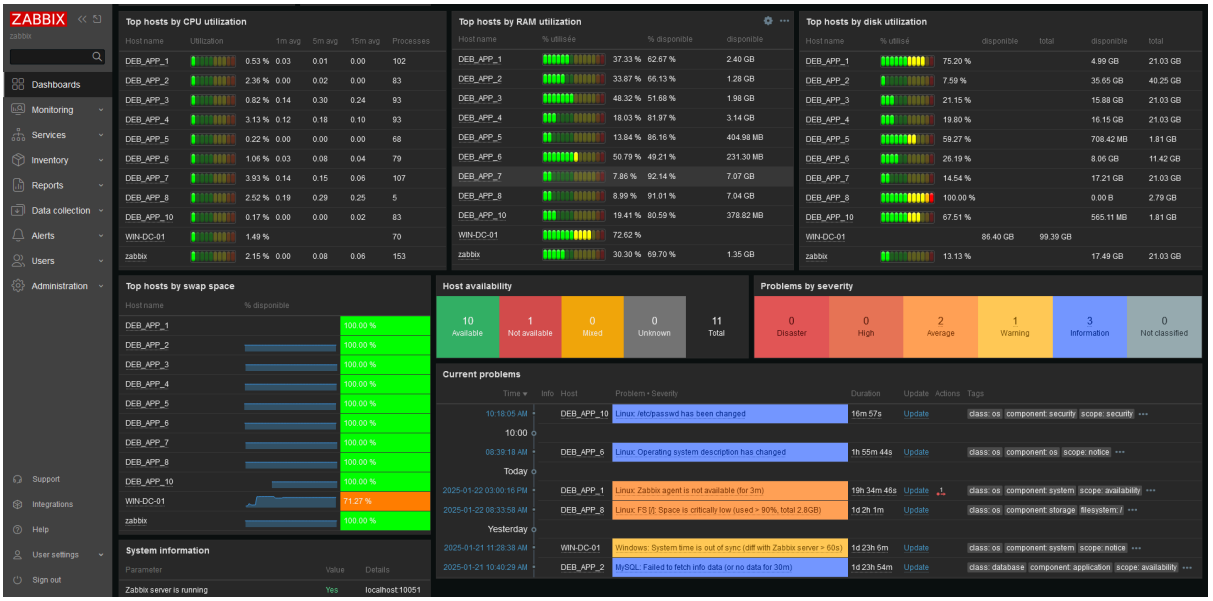
- Un serveur Zabbix dédié pour l'interface web et le traitement (10.81.110.110)
- Un serveur de base de données MariaDB distinct (10.81.110.120)
- Des agents Zabbix déployés sur chaque machine supervisée



2. Tableau de bord et monitoring

Le tableau de bord principal a été configuré pour offrir une vision instantanée de l'état de l'infrastructure avec :

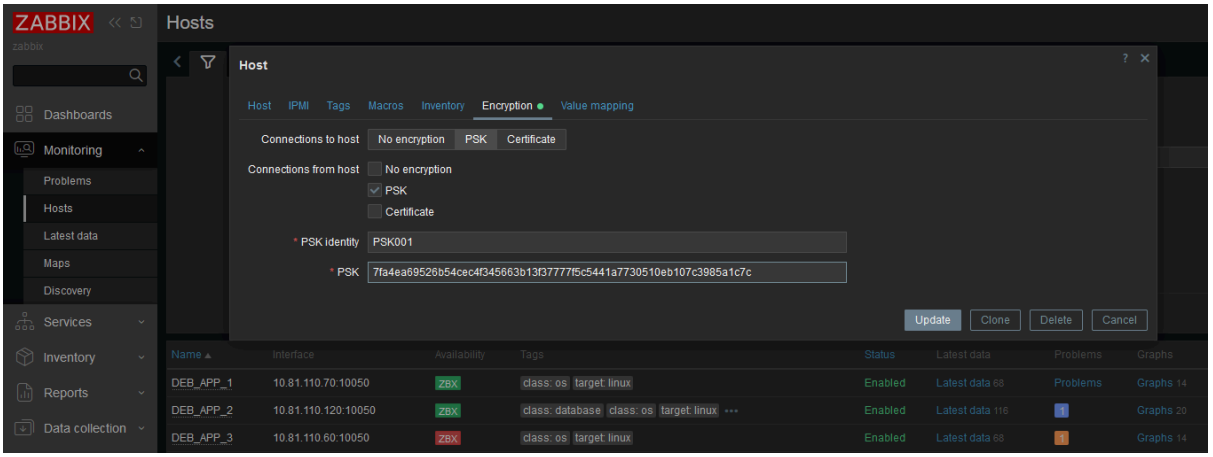
- Surveillance en temps réel de l'utilisation CPU et RAM par hôte
- Monitoring de l'espace disque et swap
- Indicateur de disponibilité réseaux des différentes machines
- Vue consolidée des problèmes par niveau de sévérité



3. Sécurisation des communications

Mise en place du chiffrement PSK (Pre-Shared Key) :

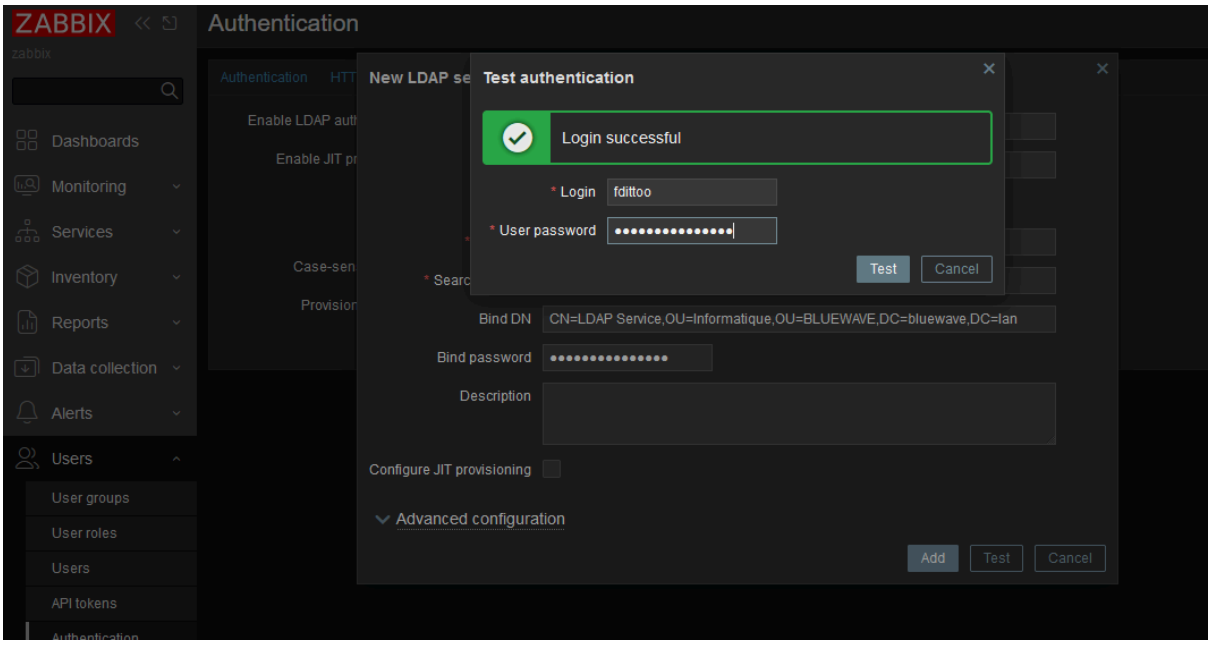
- Configuration des agents avec TLSConnect=psk et TLSAccept=psk
- Génération de clés PSK uniques pour chaque agent
- Vérification du chiffrement activé dans l'interface



4. Authentification centralisée LDAP

Intégration avec l'Active Directory :

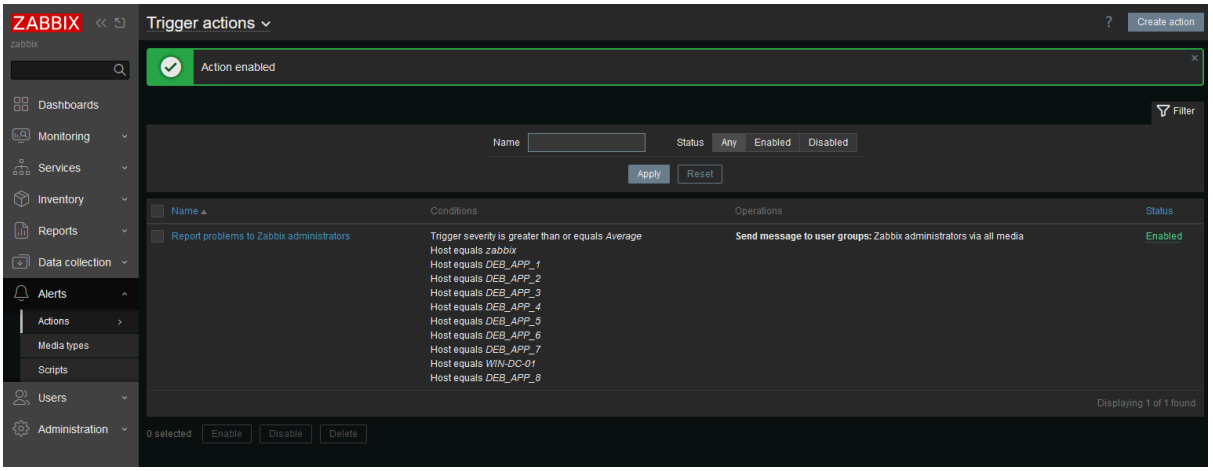
- Configuration du serveur LDAP (10.81.120.10)
- Base DN : OU=Informatique,OU=BLUEWAVE,DC=bluewave,DC=lan
- Création d'un groupe d'utilisateurs LDAP dédié dans Zabbix

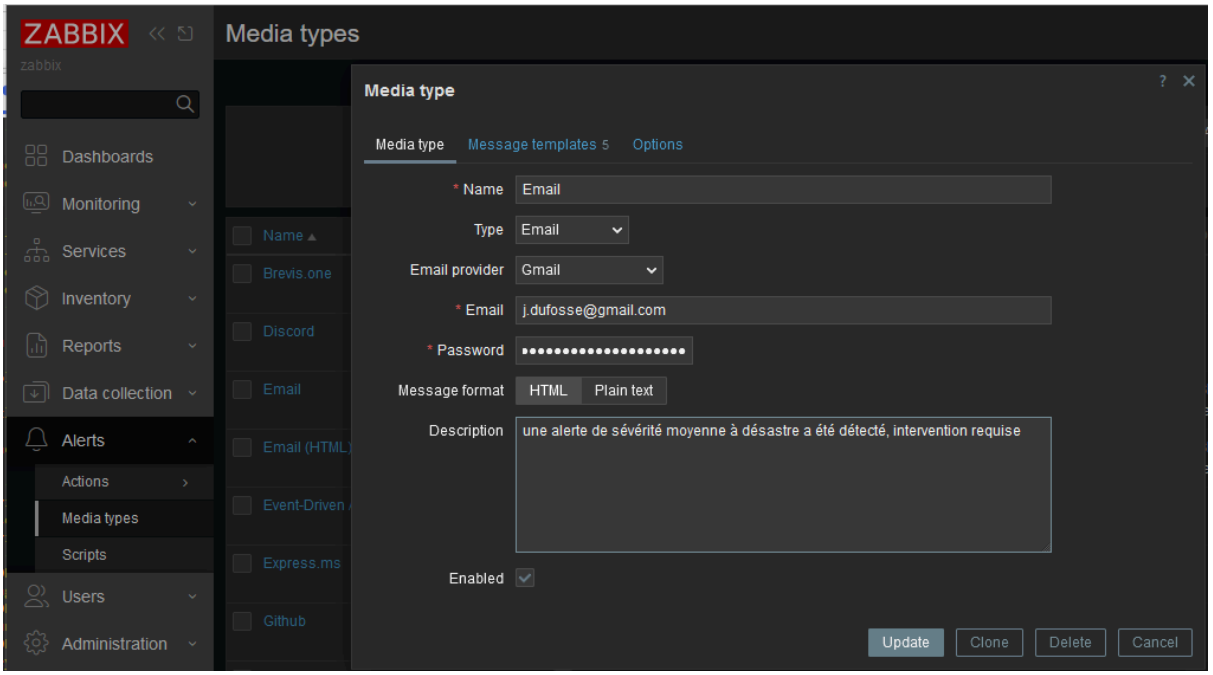


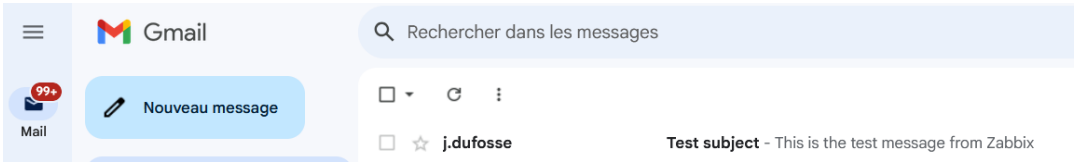
5. Système d'alertes et email

Configuration des notifications via Gmail :

- Définition des seuils d'alerte par type d'événement
- Configuration du média type Email avec Gmail
- Paramétrage des conditions de déclenchement (sévérité >= warning)
- Test de la chaîne de notification complète


ZABBIX
Trigger actions
Create action
Action enabled
Filter
Name
Status
Any
Enabled
Disabled
Apply
Reset
Name
Conditions
Operations
Status
Report problems to Zabbix administrators
Trigger severity is greater than or equals Average
Host equals zabbix
Host equals DEB_APP_1
Host equals DEB_APP_2
Host equals DEB_APP_3
Host equals DEB_APP_4
Host equals DEB_APP_5
Host equals DEB_APP_6
Host equals DEB_APP_7
Host equals WIN-DC-01
Host equals DEB_APP_8
Send message to user groups: Zabbix administrators via all media
Enabled
Displaying 1 of 1 found
0 selected
Enable
Disable
Delete
Dashboards
Monitoring
Services
Inventory
Reports
Data collection
Alerts
Actions
Media types
Scripts
Users
Administration


ZABBIX
Media types
Media type
Media type
Message templates 5
Options
* Name
Email
Type
Email
Email provider
Gmail
* Email
j.dufosse@gmail.com
* Password
Message format
HTML
Plain text
Description
une alerte de sévérité moyenne à désastre a été détecté, intervention requise
Enabled
Update
Clone
Delete
Cancel
Name
Brevis.one
Discord
Email
Email (HTML)
Event-Driven
Express.ms
Github
Dashboards
Monitoring
Services
Inventory
Reports
Data collection
Alerts
Actions
Media types
Scripts
Users
Administration


Gmail
Rechercher dans les messages
99+
Mail
Nouveau message
j.dufosse
Test subject - This is the test message from Zabbix

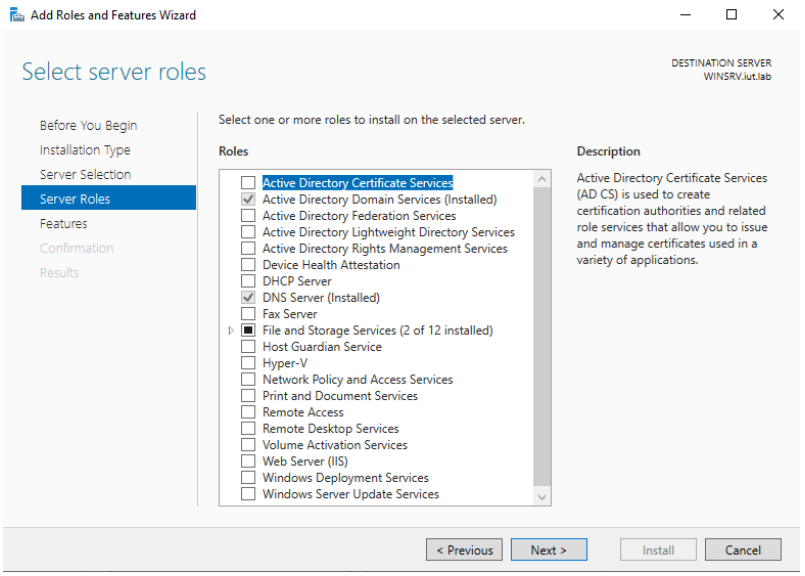
3.2. Serveurs de Services

A. Serveur Active Directory

- Installation et promotion du serveur en tant que contrôleur de domaine.

Après avoir installé Windows Server et ajouté le rôle Active Directory Domain Services (AD DS) via le Gestionnaire de serveur, nous avons promu le serveur au rôle de contrôleur de domaine. Lors de cette étape, une nouvelle forêt a été créée avec le domaine racine nommé BLUEWAVE.LAN.

3.2.1. Installation du rôle AD DS :



- Nous avons utilisé l'Assistant d'installation des rôles pour ajouter le rôle AD DS.
- Cette opération a automatiquement installé les fonctionnalités nécessaires, telles que les services DNS (si requis) et le gestionnaire AD.

3.2.2. Promotion en contrôleur de domaine :

- L'Assistant de configuration AD DS a été utilisé pour promouvoir le serveur en tant que premier contrôleur de domaine de la forêt.
- Une nouvelle forêt a été sélectionnée, et le domaine racine a été défini sur BLUEWAVE.LAN.
- Les options fonctionnelles de la forêt et du domaine ont été configurées en fonction des besoins de compatibilité (par exemple, Windows Server 2019/2022).

3.2.4. Configuration DNS :

- Si le rôle DNS n'était pas préinstallé, il a été configuré automatiquement pour permettre la résolution de noms au sein du domaine BLUEWAVE.LAN.

3.2.5. Création de l'administrateur de domaine :

- Lors de l'installation, un mot de passe de mode de restauration des services d'annuaire (DSRM) a été défini pour des interventions futures sur Active Directory.

3.2.6. Validation post-installation :

- Vérification des journaux dans l'Observateur d'événements pour confirmer la réussite de la promotion.
- Utilisation de commandes telles que dcdiag pour diagnostiquer et confirmer le bon fonctionnement du contrôleur de domaine.
- Test de la connectivité DNS et de l'enregistrement automatique des entrées SRV pour assurer la disponibilité des services AD.

>> Ces étapes garantissent une mise en œuvre robuste du premier contrôleur de domaine dans l'environnement BLUEWAVE.LAN.

- Création d'Unités d’organisation pour segmenter l'entreprise en service

Après avoir promu le serveur en tant que contrôleur de domaine et configuré la forêt **BLUEWAVE.LAN**, nous avons procédé à la création des **Unités d'Organisation (UO)** en suivant la structure topologique ci-dessous, correspondant aux services du domaine maritime :

Détails techniques de la création des UO :

3.2.7. Création des Unités d’Organisation (UO) :

- Les UO ont été créées via la console **Active Directory Users and Computers (ADUC)**.
- Chaque UO est destinée à refléter les différents services du domaine maritime, à savoir :
    - **Administratifs**
    - **Direction**
    - **Informatique**
    - **Maintenance**
    - **Marins**
- Les UO sont structurées de manière à permettre une gestion indépendante des objets (utilisateurs, groupes, ordinateurs) au sein de chaque service.

3.2.8. Commandes PowerShell utilisées pour automatiser la création :

Nous avons utilisé les commandes suivantes pour créer les UO dans un script d'automatisation :

Script pour création user et UO dans Active Directory

3.2.9. Sécurisation des UO :

- Chaque UO a été configurée avec des **droits d'administration délégués** en fonction des besoins opérationnels :
    - Les administrateurs des services respectifs ont des permissions limitées pour gérer uniquement les objets dans leur propre UO.
    - Des **politiques de délégation** ont été appliquées pour respecter les principes de moindre privilège.

3.2.10. Groupes et utilisateurs :

- Des groupes globaux ont été créés pour chaque service au sein des UO (par exemple, `GG_Admins`, `GG_Maintenance`).
- Des groupes de domaine local on aussi été créer pour créer les permission NTFS dans l'active directory (`GDL_Administratif_RW`, …)
- Les utilisateurs ont été attribués aux UO correspondantes, avec des politiques de mot de passe spécifiques appliquées via des **GPO**.

>> La hiérarchie d'Active Directory est désormais organisée pour refléter la structure fonctionnelle du domaine maritime, facilitant ainsi la gestion et l'administration centralisée des ressources et utilisateurs.

- Mise en place des GPO (Groups Policy Object) Politique de stratégie de groupe

Après la structuration des Unités d'Organisation (UO) correspondant aux services du domaine maritime, des stratégies de groupe (**GPO**) ont été configurées pour centraliser la gestion des paramètres utilisateurs et ordinateurs. Ces GPO sont adaptées aux besoins spécifiques des différents services.

3.2.11. GPO Globales pour l'ensemble du domaine BLUEWAVE.LAN

Certaines politiques ont été appliquées au niveau du domaine pour assurer une cohérence et une sécurité de base :

- **Politique de mot de passe** :
  - Longueur minimale : 12 caractères.
  - Complexité activée (majuscules, minuscules, chiffres, caractères spéciaux).
  - Expiration tous les 90 jours avec un historique des 5 derniers mots de passe.
- **Verrouillage de session** :
  - Verrouillage automatique après 10 minutes d'inactivité.
  - Message de bannière pour informer les utilisateurs des politiques de sécurité de l'entreprise.

3.2.12. GPO spécifiques par UO

a. UO Administratifs

- **Restrictions d'accès USB** :
    - Désactivation des périphériques de stockage amovibles pour éviter la fuite de données.
- **Déploiement de ressources** :
    - Mapping automatique des lecteurs réseau
    - Déploiement d'imprimantes spécifiques aux utilisateurs administratifs via **Print Management**.
    - Déploiement d'un fond d'écran

b. UO Direction

- **Renforcement de la sécurité** :
    - Utilisation de **AppLocker** pour restreindre l'exécution de logiciels non approuvés.
    - Forcer l'authentification multi-facteurs (MFA) pour tous les comptes de la direction.
- **Paramétrage des connexions** :
    - Limitation des connexions RDP aux IP internes validées.

c. UO Informatique

- **Accès administratif** :
    - Déblocage d'outils réseau et d'administration nécessaires (par exemple, PowerShell).
    - Déploiement de scripts automatisés pour la surveillance et la gestion des ressources.

- **Règles spécifiques** :
    - Activation des journaux d'événements avancés pour les diagnostics réseau.

d. UO Maintenance

- **Politiques d'économie d'énergie** :
    - Mise en veille automatique des postes après 15 minutes d'inactivité pour réduire la consommation.
- **Gestion des fichiers de rapport** :
    - Déploiement automatique des formulaires de maintenance standardisés.

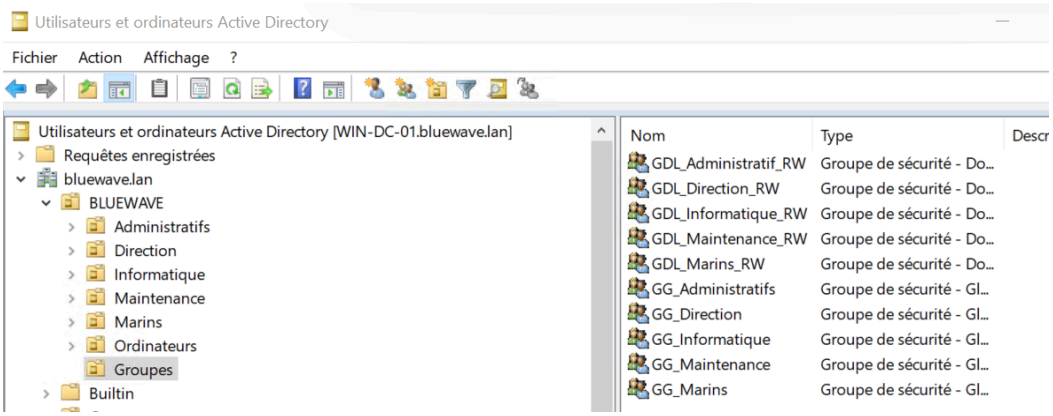
e. UO Marins

- **Sécurisation des connexions distantes** :
    - Blocage de l'accès à Internet sauf pour des sites autorisés, gérés via un proxy.
    - Forcer l'utilisation du VPN pour les connexions au domaine.
- **Ressources partagées** :
    - Création d'un dossier partagé sécurisé accessible uniquement via des sessions VPN authentifiées.

3.2.13. Création du serveur de fichier et permissions

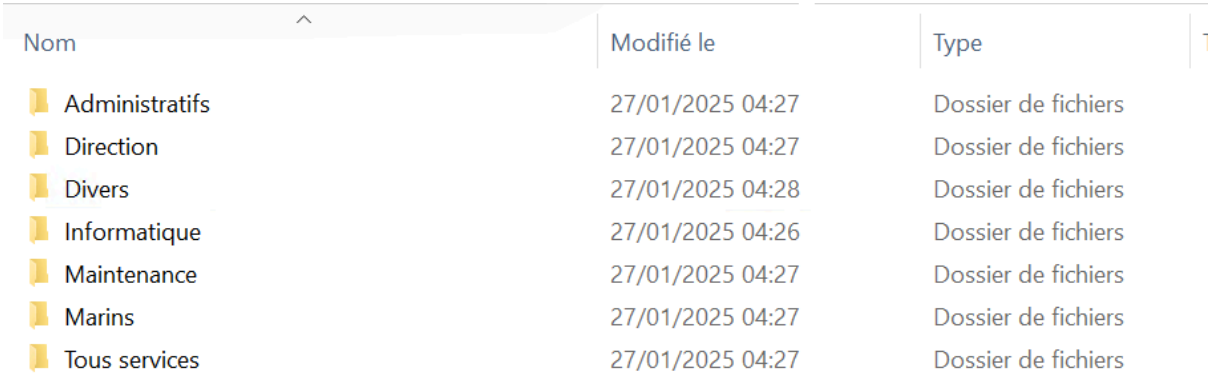
Avant de créer les répertoires à partager, nous créons des groupes de sécurité global et de domaine local, dans la capture ci-dessous. Nous voyons la mise en place de la méthode de gestion de permissions sur Windows nommée AGDLP. La méthode AGDLP consiste à appliquer le principe suivant :

- Un compte utilisateur doit être membre d'un groupe de sécurité global (GG_),
- Ce groupe de sécurité global doit ensuite être ajouté en tant que membre d'un groupe de sécurité domaine local (GDL_) - Ayant une portée uniquement sur le domaine d'appartenance,
- Ce groupe de sécurité domaine local est utilisé pour ajuster les permissions NTFS sur le répertoire partagé



Nous avons commencé par organiser les différents dossiers en fonction des services et des besoins métiers. Comme le montre la première capture, des dossiers tels que "Administratifs", "Direction", et "Maintenance" ont été créés. Cette hiérarchisation permet une séparation claire des données selon leur usage et leur sensibilité.

L'objectif ici est de simplifier la gestion tout en s'assurant que chaque service dispose de son espace dédié, avec des permissions spécifiques adaptées.

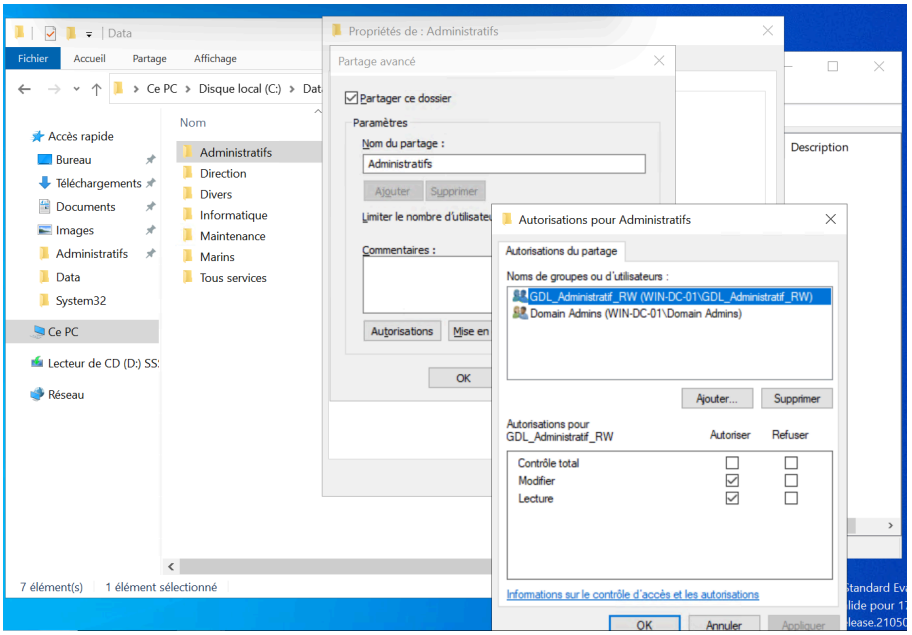


Nom	Modifié le	Type
Administratifs	27/01/2025 04:27	Dossier de fichiers
Direction	27/01/2025 04:27	Dossier de fichiers
Divers	27/01/2025 04:28	Dossier de fichiers
Informatique	27/01/2025 04:26	Dossier de fichiers
Maintenance	27/01/2025 04:27	Dossier de fichiers
Marins	27/01/2025 04:27	Dossier de fichiers
Tous services	27/01/2025 04:27	Dossier de fichiers

Une fois les dossiers créés, nous avons configuré les droits d'accès pour chaque répertoire. En prenant l'exemple du dossier **"Administratifs"** (capture suivante) :

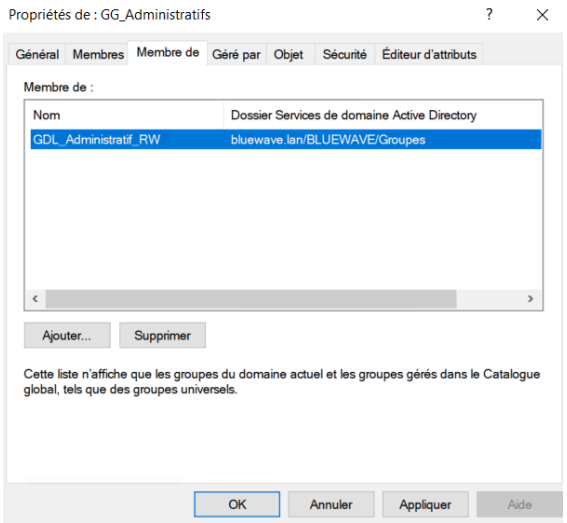
- **GDL_Administratif_RW** : Ce groupe dispose de droits de lecture et d'écriture, permettant aux membres de modifier les fichiers.
- **Domain Admins** : Réservé aux administrateurs pour une gestion technique et administrative.

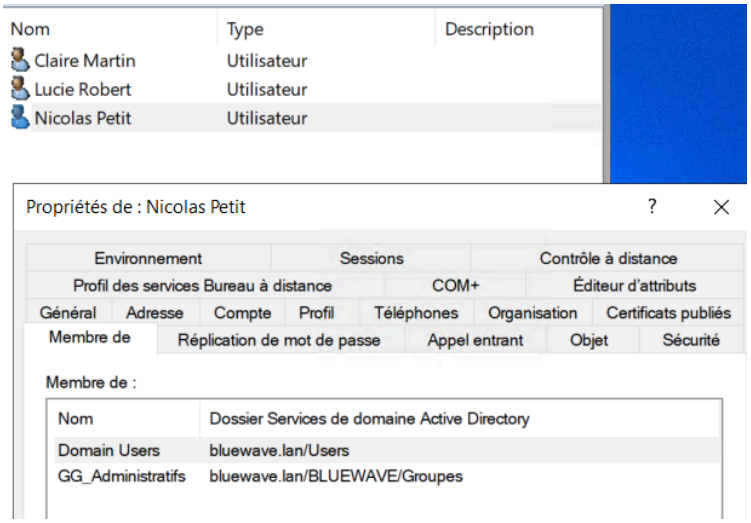
Cette méthode repose sur l'utilisation des groupes Active Directory pour centraliser et simplifier la gestion des droits.



La troisième étape a consisté à rattacher les utilisateurs aux groupes adéquats. Comme illustré dans la troisième capture, nous avons ajouté des utilisateurs au groupe **GG_Administratifs**, lequel est ensuite lié au groupe **GDL_Administratif_RW**.

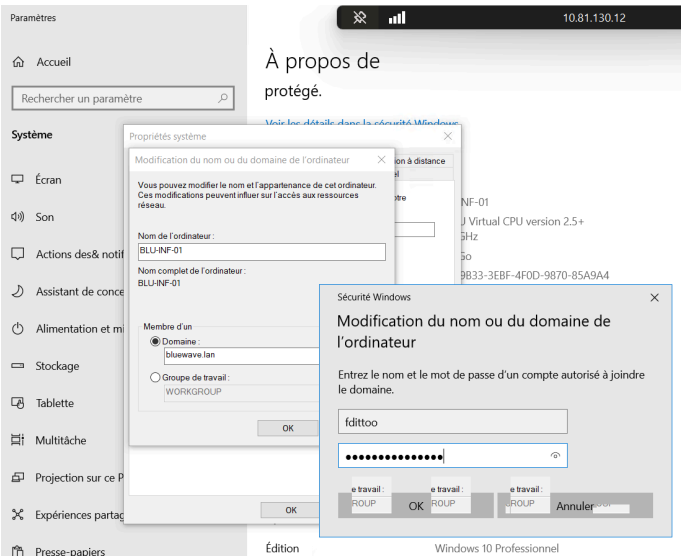
Cette hiérarchie permet une gestion modulaire : en modifiant les droits d'un groupe, nous affectons automatiquement tous ses membres. Cela réduit les risques d'erreur humaine et facilite les modifications à l'avenir.

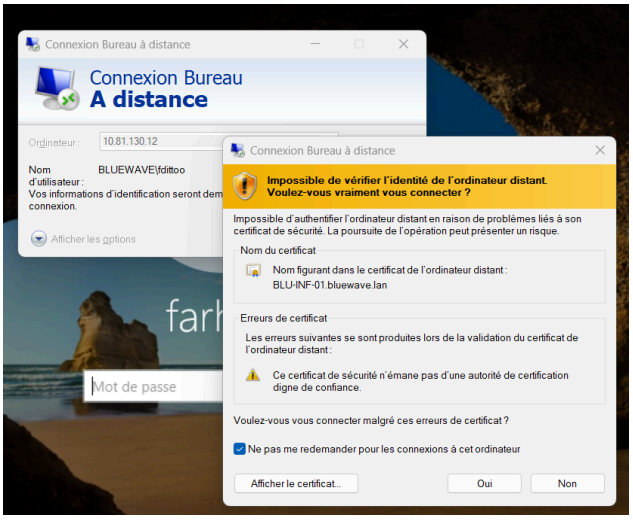




Une fois les configurations terminées, nous avons vérifié que les droits sont bien appliqués. Dans la dernière capture, nous voyons que l'utilisateur **thomas.blanc** a pu accéder sans problème au dossier partagé "Informatique" via le serveur **win-dc-01**, que celui n'ai pas accés à d'autre partage.

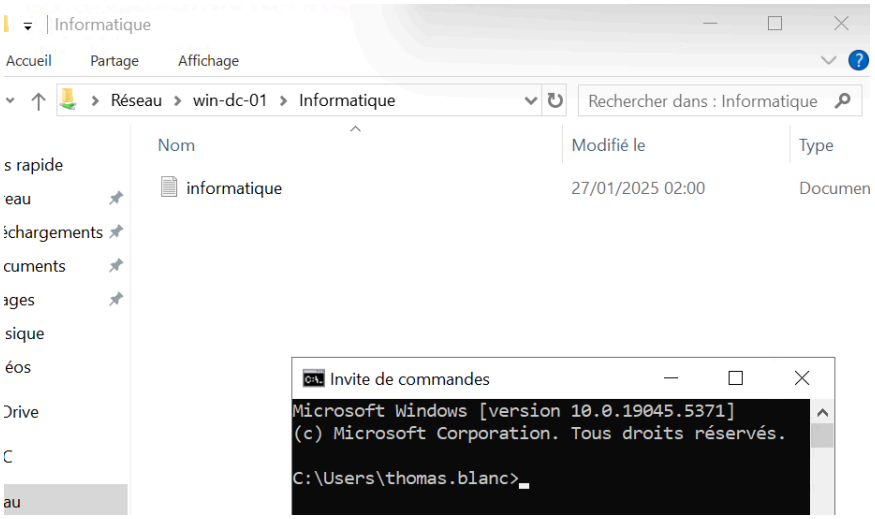
Il s'agit ensuite de rejoindre le domaine Active Directory avec les postes clients. Pour ce faire, dans les paramètres avancés du système, nous quittons le groupe de travail (workgroup) et intégrons le domaine **bluewave.lan**.

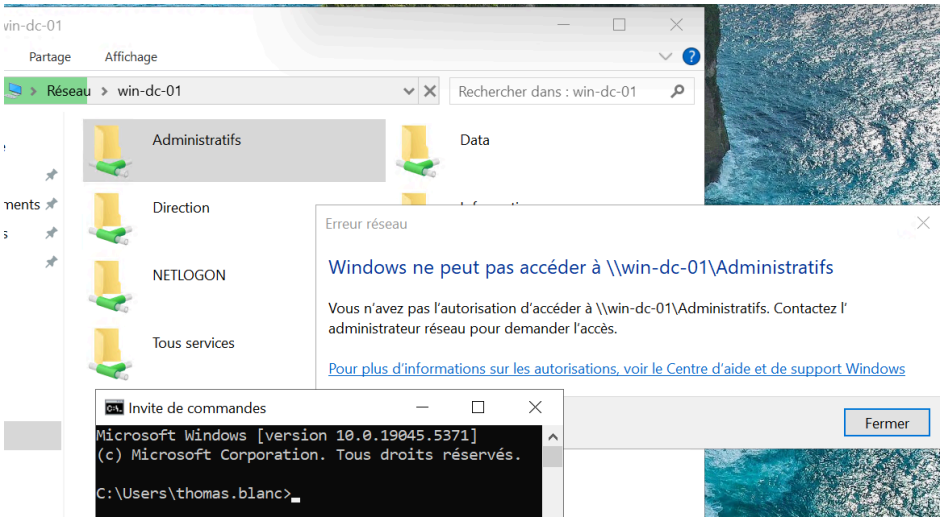




Après cela, et une fois le mappage des lecteurs effectué via GPO, nous pouvons constater que les lecteurs sont bien montés. Les utilisateurs ont accès uniquement aux dossiers auxquels ils sont autorisés.

Cette vérification garantit que les permissions définies sont fonctionnelles et conformes aux besoins des utilisateurs tout en respectant les règles de sécurité.





Ce déroulé met en évidence les étapes essentielles pour mettre en place une gestion efficace des dossiers partagés dans un environnement Windows Server. En structurant les dossiers, en configurant les permissions via Active Directory, et en vérifiant les accès, nous assurons une organisation optimale et sécurisée des données, adaptée aux besoins des différents services de l'entreprise.

3.3. Durcissement d'AD

Harden AD (outil de durcissement Active Directory) facilite la sécurisation d'une infrastructure AD en proposant des configurations automatisées pour les meilleures pratiques de sécurité. Voici une procédure intégrant Harden AD

3.4.1. BackUp de Active Directory

- Installation :

Ouvrir Gestionnaire de serveur > Ajouter des rôles et fonctionnalités > Cocher Windows Server Backup > Installer.

- Sauvegarde Planifiée :

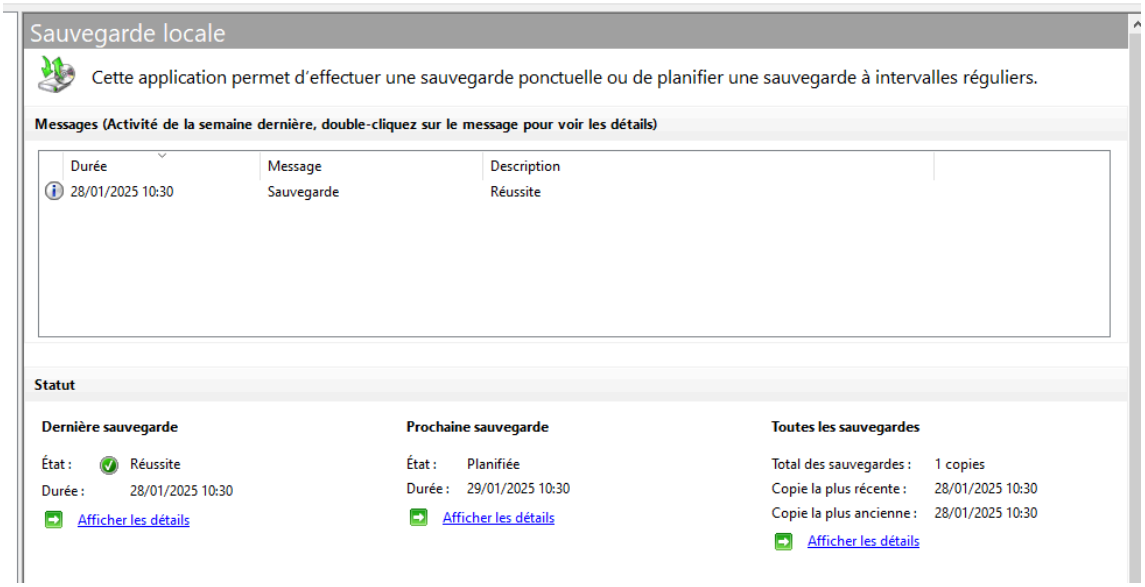
Ouvrir Windows Server Backup (wbadmin.msc) > Planifier une sauvegarde.

Choisir Sauvegarde personnalisée > Ajouter État du système.

Planifier la fréquence > Sélectionner la destination > Valider.

- Vérification :

Vérifier l'historique dans Sauvegardes locales pour s'assurer du succès.




```
C:\Users\Administrator>repadmin /showbackup

Repadmin : exécution de la commande /showbackup sur le contrôleur de domaine complet localhost

USN loc                          DSA source       USN org. Heure/date org.      Attribut ver
=======                          ==========       ======== ===========      === ========
DC=ForestDnsZones,DC=bluewave,DC=lan
  78644      6c9d5101-13f5-45ab-80df-d7ec3be69a42     78644 2025-01-28 10:33:33    2 dSASignature
DC=DomainDnsZones,DC=bluewave,DC=lan
  78643      6c9d5101-13f5-45ab-80df-d7ec3be69a42     78643 2025-01-28 10:33:33    2 dSASignature
CN=Schema,CN=Configuration,DC=bluewave,DC=lan
  78642      6c9d5101-13f5-45ab-80df-d7ec3be69a42     78642 2025-01-28 10:33:33    2 dSASignature
CN=Configuration,DC=bluewave,DC=lan
  78641      6c9d5101-13f5-45ab-80df-d7ec3be69a42     78641 2025-01-28 10:33:33    2 dSASignature
DC=bluewave,DC=lan
  78640      6c9d5101-13f5-45ab-80df-d7ec3be69a42     78640 2025-01-28 10:33:33    2 dSASignature
```

3.3.2.Harden AD

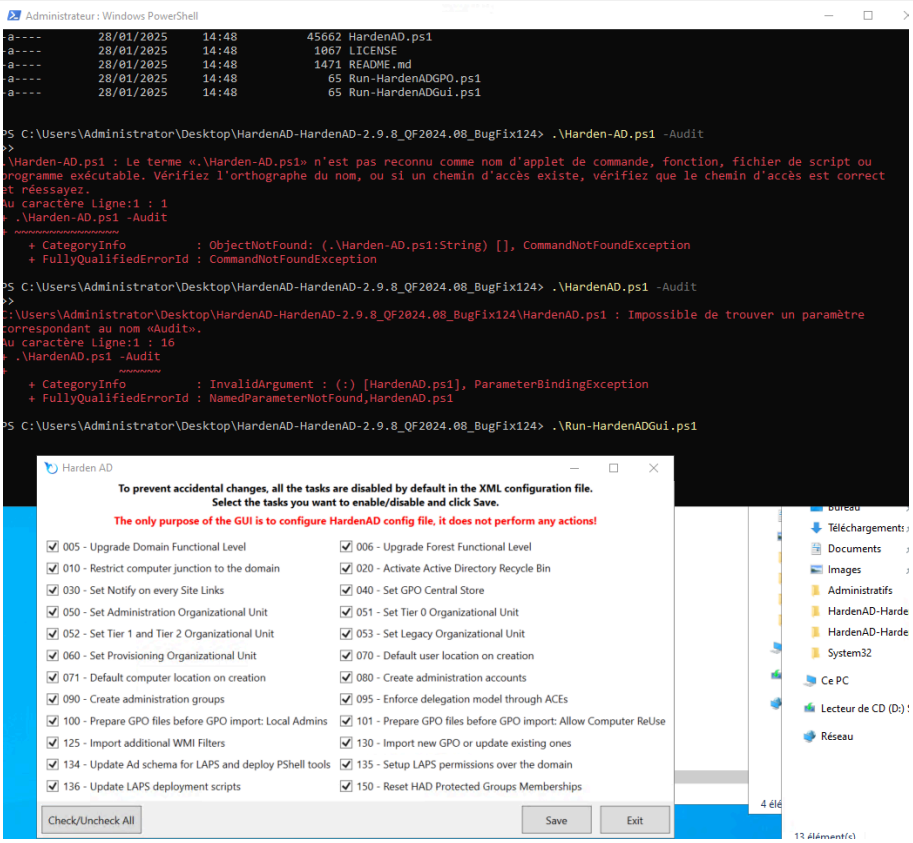
Procédure de Durcissement Active Directory avec Harden AD

Prérequis

- Télécharger et installer Harden AD depuis le GitHub officiel.
- Vérifier que PowerShell est installé avec les permissions administratives nécessaires.
- Assurer une sauvegarde complète de l'Active Directory et des contrôleurs de domaine.

Nous exécutons la commande ci-dessous afin de sélectionner les options que l'on voulons activer pour démarrer l'Hardening:

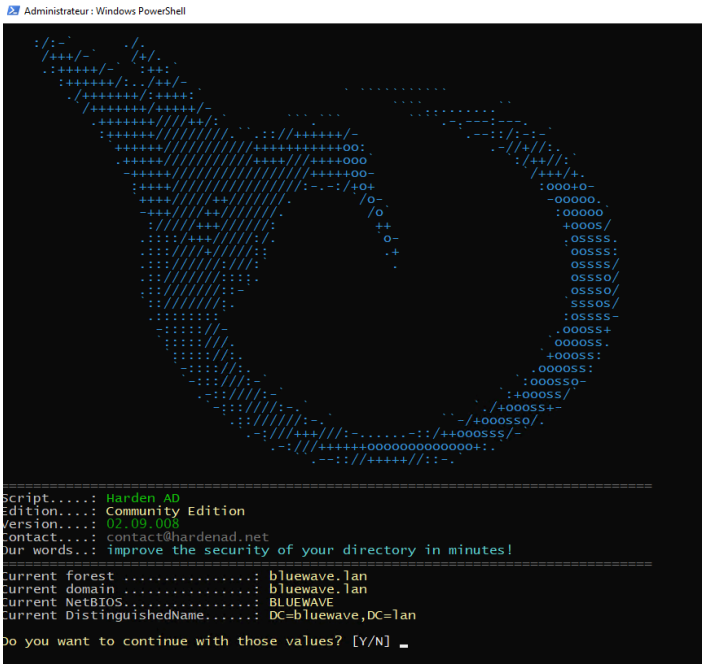
```
.\Harden-ADGUIps1 -Audit
```

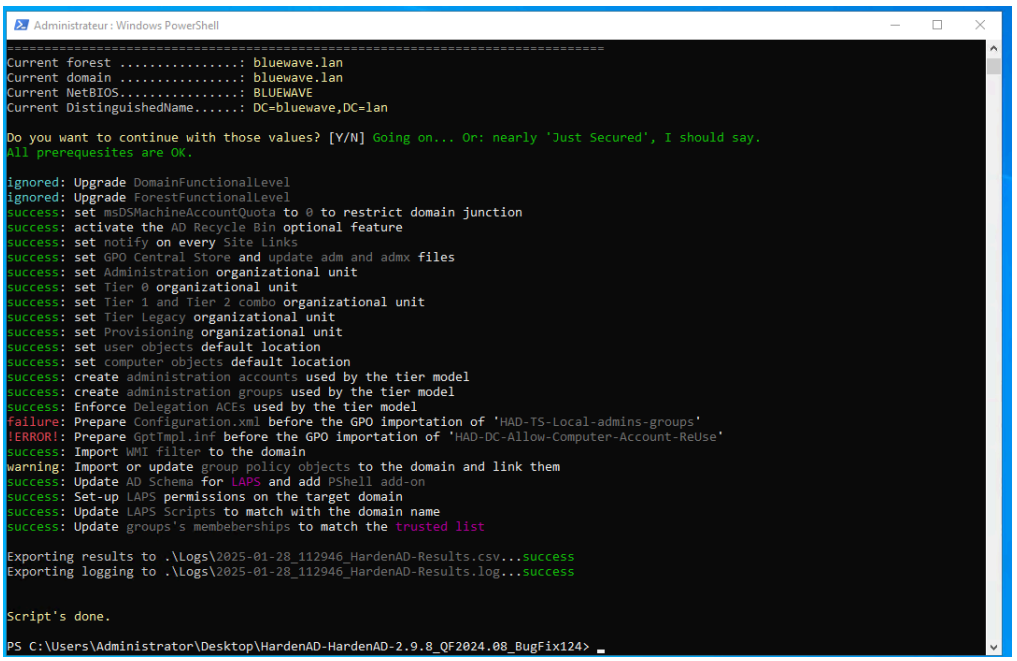


Une fois terminée, nous éxécutons la commande ci-dessous pour lancer le début de l'Hardening de L'Active Directory

```
.\Harden-AD.ps1
```

Nous voyons dans le screen ci-dessous la sélection de notre Active Directory à savoir bluewave.lan





- **Mise à niveau des niveaux fonctionnels** :
    - Domaine et forêt à **Windows 2016**, déjà à jour donc aucune modification nécessaire.

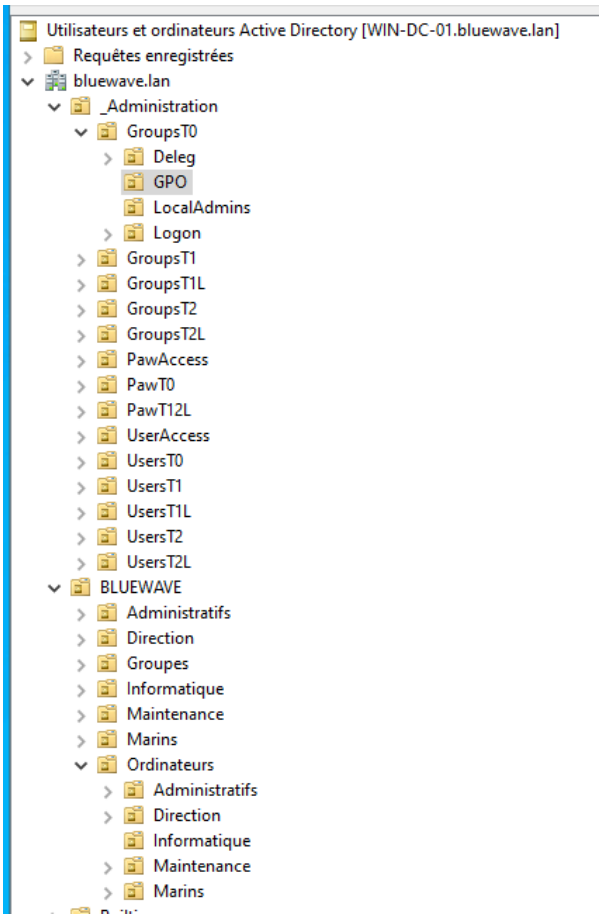
- **Restrictions et configurations de sécurité** :
    - Restriction des jonctions d'ordinateurs au domaine (`msDSMachineAccountQuota`).
    - Activation de la **corbeille Active Directory** pour restaurer les objets supprimés.
    - Notification sur chaque lien de site configurée.
- **Organisation hiérarchique** :
    - Mise en place des **Unités Organisationnelles (OU)** selon une architecture bien définie (Administration, Tier 0, Tier 1/2, Legacy, Provisionning).
- **Paramétrages par défaut** :
    - Définition des emplacements par défaut pour les nouveaux utilisateurs et ordinateurs.
- **Sécurisation des comptes administratifs** :
    - Création de **comptes administratifs** et de **groupes d'administration**.
    - Application d'un modèle de délégation via des ACE (Access Control Entries).
- **Préparation des GPO (Group Policy Objects)** :
    - Importation de fichiers pour configurer les administrateurs locaux.

Points à vérifier

- Les tâches `Upgrade Domain Functional Level` et `Upgrade Forest Functional Level` ont été ignorées car les niveaux étaient déjà au plus haut possible (Windows 2016). Cela peut indiquer une infrastructure déjà optimisée à ce niveau.
- Il serait intéressant de confirmer si la mise en place de l'arborescence des OU (comme `HardenAD_ADMIN` ou `HardenAD_PROD`) correspond bien aux recommandations en matière de sécurité.

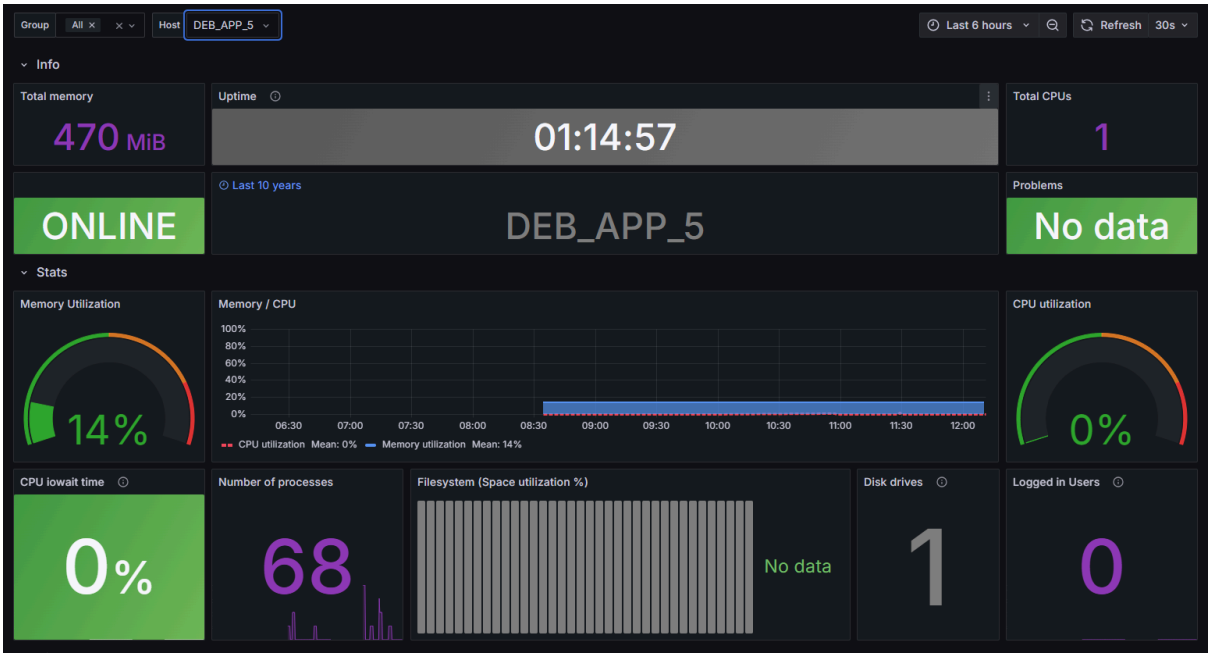
Bonnes pratiques observées

- Activation de la corbeille Active Directory, qui est une fonction précieuse en cas d'erreur de suppression.
- Mise en place des niveaux Tier pour l'isolement des rôles administratifs, une mesure couramment adoptée pour durcir la sécurité d'AD.
- Gestion fine de la délégation des permissions grâce aux ACE.



Nous voyons la différence entre notre annuaire avant et après l'Hardening avec cette étape de sécurisation nous avons perdu un totale de 10 points sur notre rapport pingCastle.

C. Grafana



- **Connecté au SOC :**
  - Intégré aux outils SOC pour surveiller les **métriques essentielles** des serveurs (CPU, RAM, trafic réseau, etc.).
- **Dashboards personnalisés :**
  - Configuration de **tableaux de bord dynamiques** pour une visualisation claire et rapide des performances.
- **Alertes proactives :**
  - Définition de seuils critiques (par exemple, utilisation CPU > 80 %, RAM > 90 %, trafic réseau anormal).
  - Les dépassements de ces seuils génèrent des **alertes immédiates**, permettant une intervention rapide.

3.3. Serveurs de la Zone Front

A. webterm-1 (Docker)

- **Utilisation de conteneurs Docker** :

  Ce serveur utilise une architecture conteneurisée pour garantir une isolation efficace et simplifier la gestion des applications hébergées.
- **Configuration sécurisée** :
  - Héberge un environnement WordPress dédié aux tests d'audit de sécurité.
  - Accessible via HTTPS avec des certificats TLS pour assurer la confidentialité et l'intégrité des communications.

B. Windows10-1 & Windows10-2

- **Poste de travail pour tests** :

  Ces machines sont utilisées pour tester des applications ou réaliser des configurations spécifiques dans un environnement contrôlé.
- **Limitation des accès** :
  - Configurées pour ne pas interférer avec les autres serveurs ou services critiques de la zone.

C. Web-Server

- **Hébergement d'applications web** :

  Ce serveur est dédié à l'hébergement d'applications publiques et internes, avec un accent mis sur la sécurité.
- **Pare-feu applicatif (WAF)** :

  Protège contre les attaques courantes telles que :
  - Injection SQL
  - Cross-Site Scripting (XSS)
  - Autres vulnérabilités des applications web
- **HTTPS activé avec certificat TLS** :

  Toutes les connexions sont chiffrées pour garantir la protection des données échangées.

D. Proxy inversé

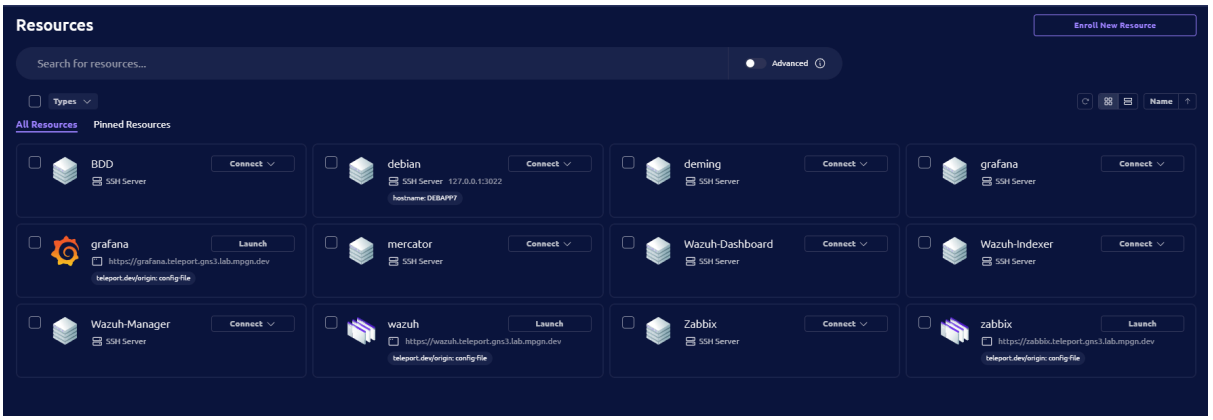
- **Redirection des connexions entrantes** :

  Filtre les requêtes provenant du réseau WAN et les redirige uniquement vers les services autorisés.
- **Filtrage des requêtes suspectes** :

  Empêche les tentatives d'attaques ou les connexions non autorisées d'atteindre les serveurs internes, renforçant ainsi la sécurité de la zone Front.

3.3. Bastion

Le bastion est configuré avec **Teleport (10.81.140.50)**, une solution d'accès sécurisé centralisé pour les administrateurs. Il sert de point d'entrée unique pour gérer et superviser l'infrastructure tout en assurant une traçabilité et une sécurité renforcées.



Fonctionnalités principales de Teleport :

1. **Accès centralisé sécurisé :**
    - Permet aux administrateurs de se connecter à tous les systèmes via une interface unique.
    - Trafic entièrement chiffré (SSH/TLS).
2. **Authentification renforcée :**
    - **MFA (Multi-Factor Authentication)** obligatoire pour tous les utilisateurs.

3. **Audit et traçabilité :**
    - Journalisation complète des sessions (SSH, RDP).
    - Enregistrements des commandes exécutées et des fichiers transférés.
    - Alertes en temps réel pour les tentatives de connexion non autorisées.
4. **Proxy unique :**
    - Redirection des connexions vers les serveurs cibles en fonction des permissions accordées.
    - Proxy HTTPS pour les connexions SSH et RDP.

Les accès sont gérés de manière fine, permettant à chaque membre de l'entreprise d'accéder uniquement aux serveurs qui lui sont attribués. (Voir l'annexe pour la configuration)

4. Audit de sécurité

L'audit de sécurité est un processus clé pour garantir la résilience des systèmes d'information, identifier les vulnérabilités et évaluer l'efficacité des mesures de protection en place. Voici les étapes et objectifs principaux :

4.1. Objectifs de l'audit :

1. **Évaluation des configurations :**
    - Vérifier que les serveurs (SOC, Services, Front) respectent les bonnes pratiques de sécurité.
    - S'assurer que les composants critiques (pare-feu, WAF, Active Directory, CrowdSec, etc.) sont correctement configurés.
2. **Détection des vulnérabilités :**
    - Identifier les points faibles dans les systèmes, les applications et les configurations réseau.
    - Analyser les accès non autorisés ou les comportements suspects.
3. **Test des politiques de sécurité :**
    - Vérifier la robustesse des politiques comme la gestion des mots de passe, l'authentification MFA et les GPO.
    - S'assurer de l'application des règles de segmentation réseau (par exemple, isolation des zones SOC, Services, et Front).

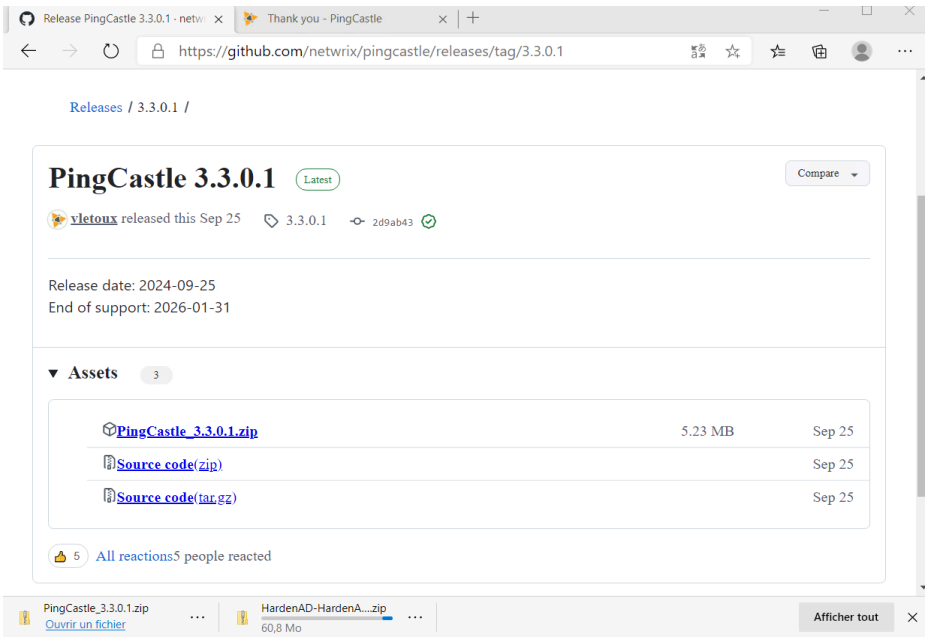
4. **Simulation d'attaques :**
    - Réaliser des tests de pénétration (Pentest) pour évaluer la capacité des systèmes à résister à des menaces ciblées, telles que les attaques réseau ou applicatives.
5. **Validation des mécanismes de remédiation :**
    - Vérifier que les mécanismes comme CrowdSec, le WAF, et les alertes Grafana détectent et répondent efficacement aux incidents.

4.2. Ping Castle avant l'Hardening

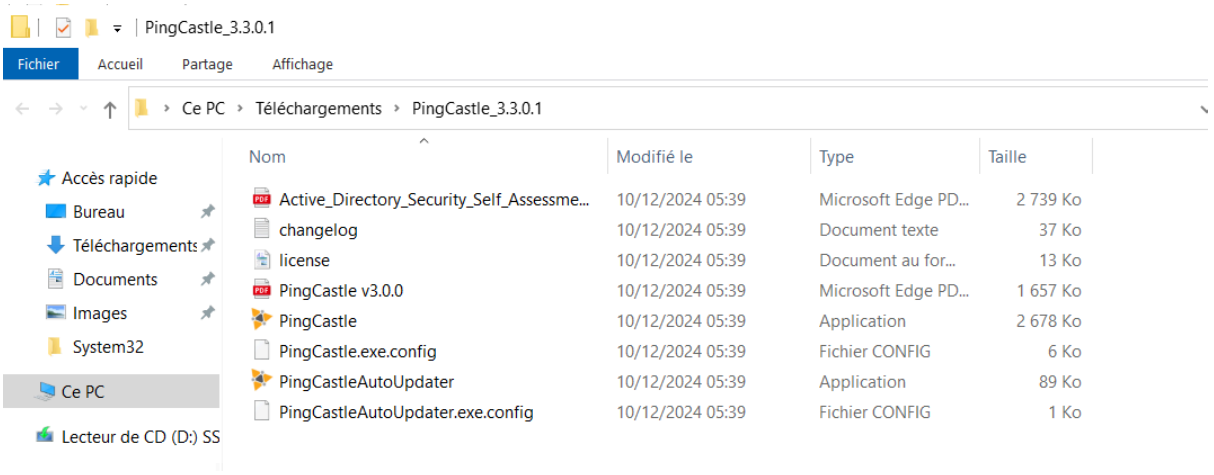
Procédure pour faire un audit avec PingCastle :

1. Télécharger PingCastle

- Rendez-vous sur le site officiel de PingCastle et téléchargez la dernière version de l'outil.

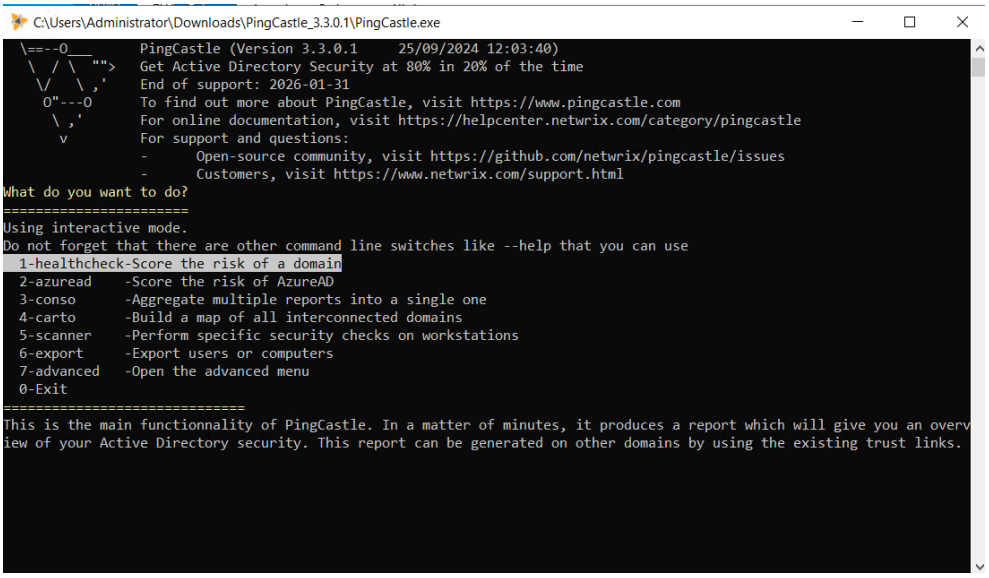


- Extrayez le contenu de l'archive téléchargée sur une machine (de préférence un serveur ou un poste de travail dans le domaine Active Directory à auditer).



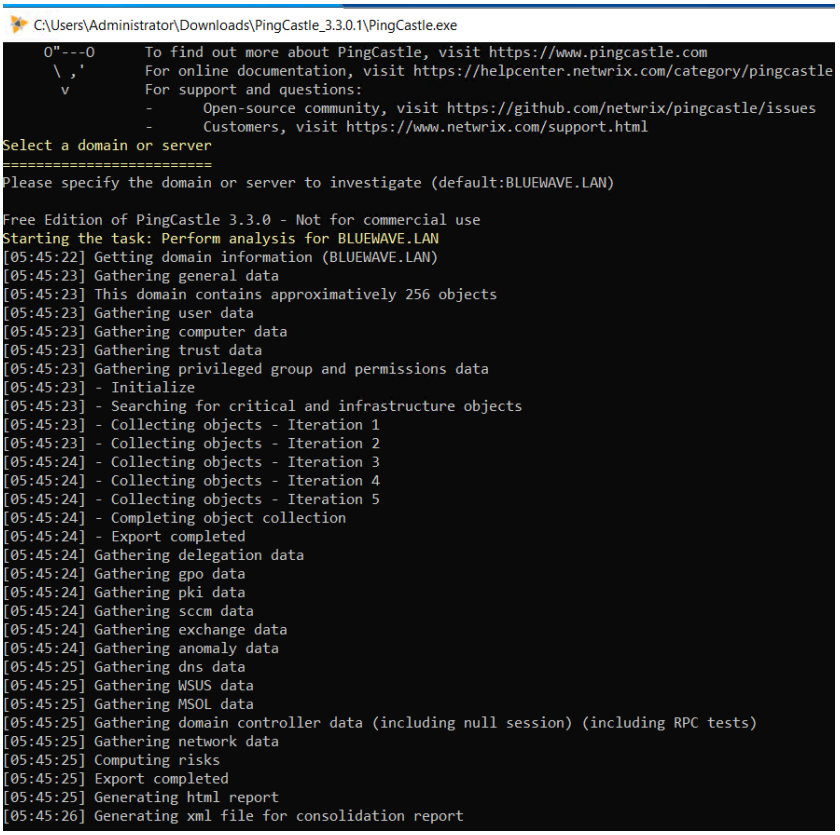
2. Exécuter PingCastle en tant qu'administrateur

- Ouvrez une fenêtre **PowerShell** ou **Invite de commandes** en mode administrateur.
- Accédez au répertoire où vous avez extrait PingCastle.



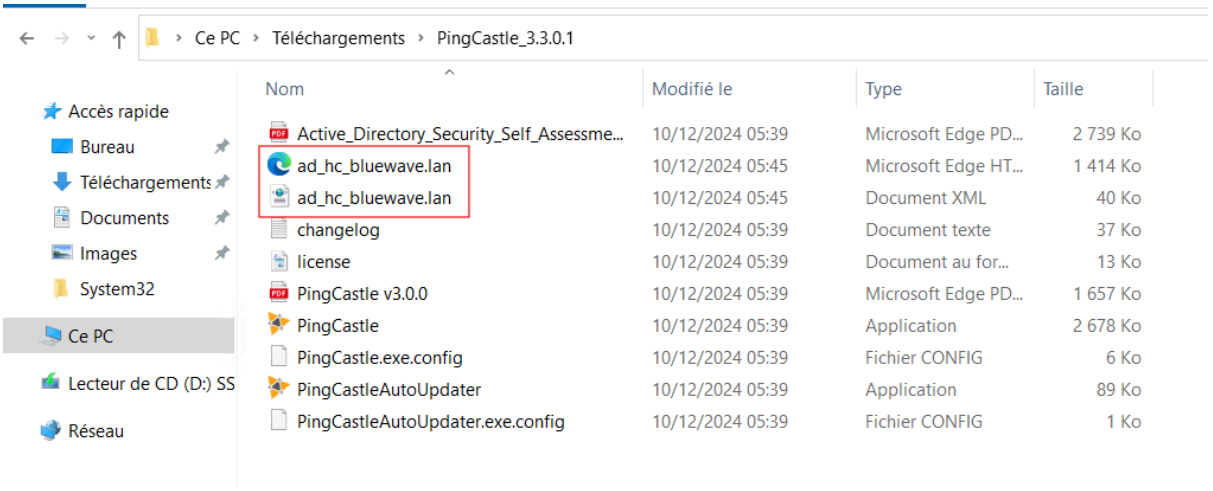
3. Choisir le mode d'audit

PingCastle propose plusieurs modes d'audit en fonction des besoins. Par défaut, le mode **HealthCheck** sera utilisé pour un audit de base, mais vous pouvez aussi spécifier d'autres options comme un audit spécifique sur les vulnérabilités AD :

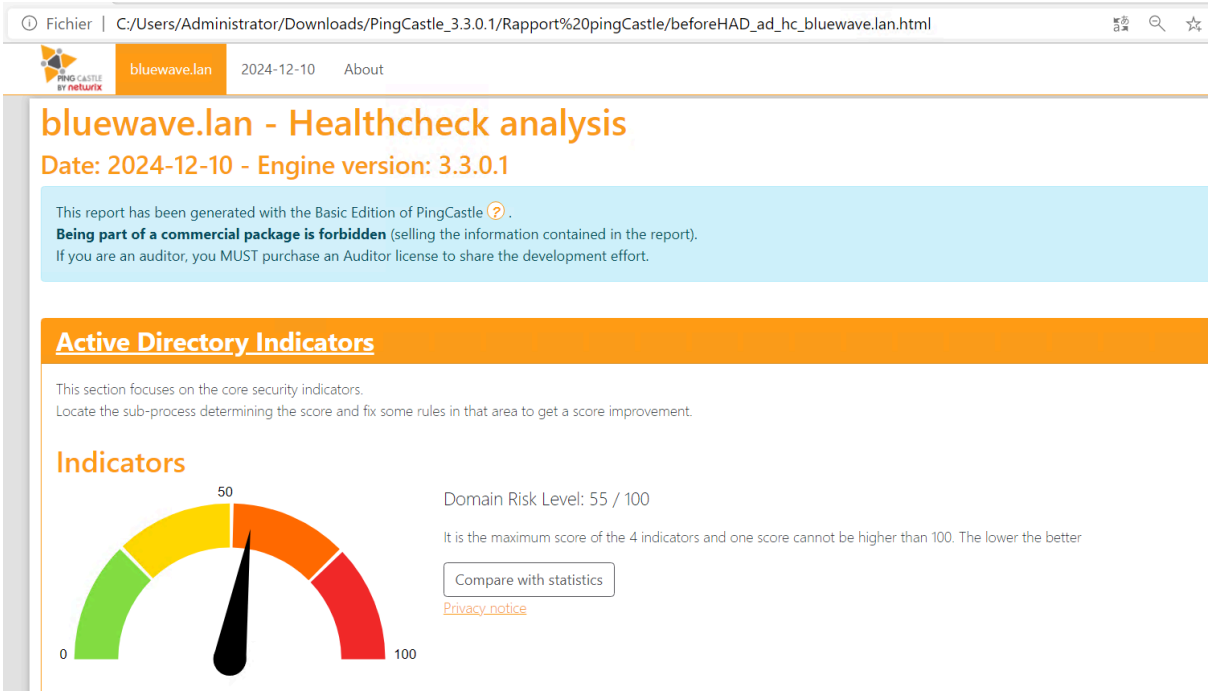


4. Analyser les résultats

Une fois l'audit effectué, PingCastle génère un rapport au format HTML dans le même dossier où l'exécutable se trouve. Le fichier est généralement nommé `report_XXXX.html` (XXXX correspond à la date/heure).



- Ouvrez le fichier HTML dans votre navigateur pour examiner les résultats.
- Le rapport présente plusieurs sections avec des indicateurs de santé pour différents aspects d'Active Directory, tels que :
    - **Comptes utilisateurs et groupes vulnérables**
    - **Stratégies de mot de passe**
    - **Permissions excessives sur les objets**
    - **Présence de comptes administrateurs ou services obsolètes**
    - **Sécurité des contrôleurs de domaine**



Les points faibles sont identifiés et classés par priorité.

5. Réagir aux résultats

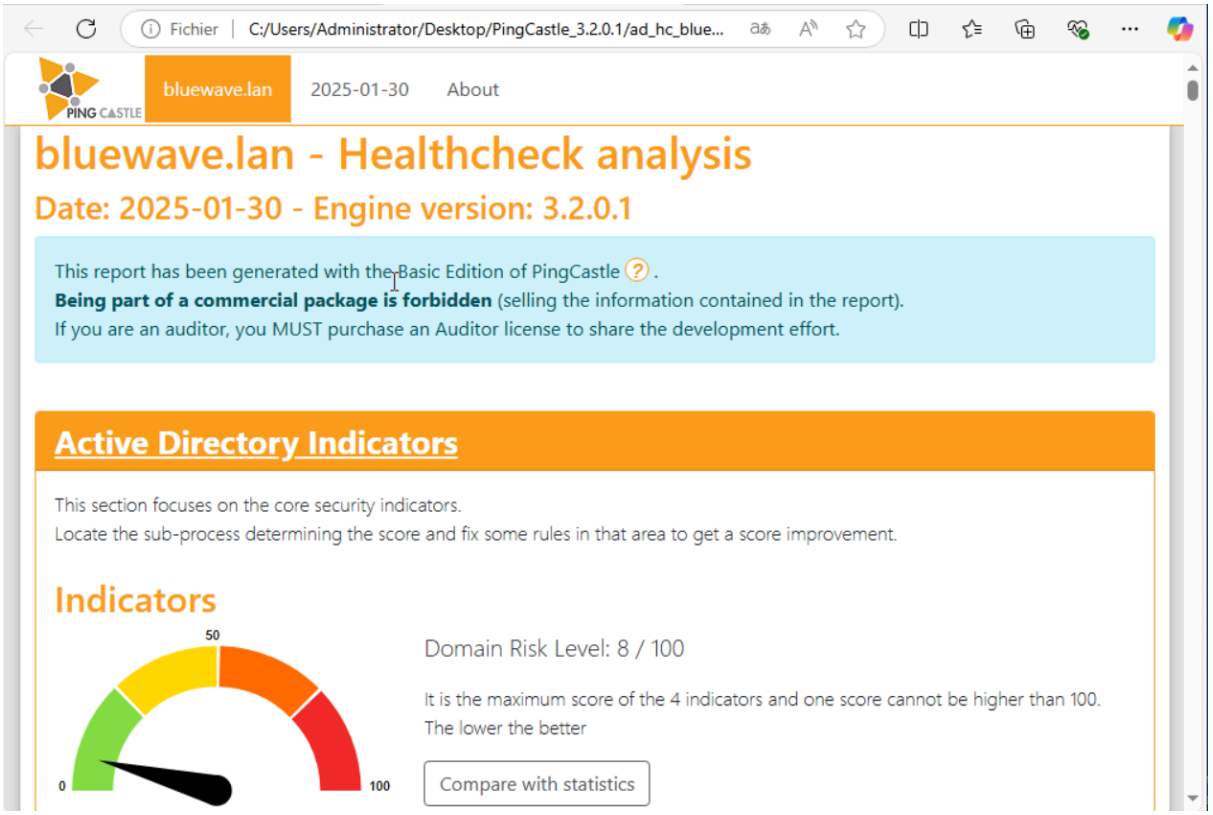
- Analysez les recommandations faites par PingCastle pour chaque vulnérabilité identifiée.
- Appliquez les correctifs nécessaires dans votre environnement Active Directory, en particulier pour les points de sécurité critiques comme la gestion des comptes et les stratégies de mot de passe.

PingCastle est un outil puissant qui permet de repérer une grande variété de vulnérabilités sur un Active Directory. Il est particulièrement utile pour évaluer la posture de sécurité de l'AD et pour détecter les mauvaises configurations ou pratiques.

4.3. Ping Castle après l'Hardening

Suite à la phase de sécurisation et d'implémentation des mesures d'hardening sur l'infrastructure Active Directory, une analyse complémentaire a été effectuée à l'aide de **Ping Castle**. Cet outil d'audit est particulièrement utile pour évaluer la posture de sécurité d'un domaine Active Directory en mettant en lumière les failles potentielles et les configurations à risque.

L'objectif de cette étape était de vérifier l'efficacité des mesures d'hardening précédemment mises en place et de s'assurer que les principales vulnérabilités avaient été atténuées. Les captures d'écran ci-dessous illustrent les résultats obtenus et permettent d'analyser les améliorations constatées ainsi que les éventuels points de vigilance restant à traiter.



4.4. Audit d'un site web Wordpress

1. Contexte et Objectifs

1.1 Contexte

Le site web de Blue Wave Logistics constitue une interface publique critique pour ses clients, partenaires et employés. Conçu pour fournir des services stratégiques et opérationnels, ce site doit respecter des standards élevés en matière de sécurité. Une faille pourrait entraîner :

- Des pertes financières importantes,

- Une atteinte à la réputation de l'entreprise,

- Un risque de non-conformité réglementaire.

1.2 Objectifs

L'audit visait à :

- Identifier les vulnérabilités critiques, telles que les injections SQL, les failles XSS, et les problèmes d'authentification.

- Simuler des attaques pour évaluer la résilience du système face à des menaces réelles.

- Fournir des recommandations concrètes et applicables pour améliorer la posture de sécurité du site.

2. Méthodologie

2.1 Phases d'audit

1. Reconnaissance :

- Identification des ports et services ouverts via Nmap.

Détails de l'hôte :

1. Adresse IP : 192.168.50.197

o Il s'agit d'une adresse IP privée, utilisée dans un réseau local (probablement une machine virtuelle ou un environnement de test vu la MAC address VMware).

2. Latence : 0.00064s

o La latence extrêmement basse indique que l'hôte est très proche sur le réseau, typiquement dans le même réseau local.

3. MAC Address : 00:0C:29:AC:5C:24

o Le préfixe indique que la machine tourne sur une virtualisation VMware.

Ports ouverts :

1. Port 22 (SSH)

- État : Ouvert
- Service : SSH (Secure Shell)

o Cette version est associée à Debian Squeeze, une distribution obsolète, et est vulnérable à des failles connues, notamment :

CVE-2010-4478 (Fuite de mémoire).

CVE-2016-3115 (Contournement des restrictions d'accès).

o Si ce port est exposé sur Internet, il est crucial de :

Désactiver les méthodes d'authentification non sécurisées comme l'authentification par mot de passe.

Mettre à jour OpenSSH ou restreindre l'accès à des adresses IP spécifiques via un pare-feu.

---

2. Port 80 (HTTP)

- État : Ouvert
- Service : HTTP
- Version : Apache 2.2.16 ((Debian))

o Cette version d'Apache est obsolète et non sécurisée. Elle peut présenter des vulnérabilités telles que :

CVE-2011-3192 : Vulnérabilité d'épuisement de mémoire (DoS) via des requêtes HTTP malformées.

CVE-2010-1452 : Attaque par inclusion de fichiers.

o Ce service semble être utilisé pour héberger une page ou une application web (comme suggéré dans le précédent rapport). La configuration HTTP doit être examinée, et des tests approfondis de sécurité doivent être effectués (par exemple, avec Nikto, Dirb, ou OWASP ZAP).

<u>Informations sur le système :</u>

- OS : Linux

o Le système d'exploitation semble être une version de Linux associée à Debian 6 (Squeeze), une distribution obsolète, qui n'est plus maintenue depuis 2016. Cela représente un risque majeur, car de nombreuses vulnérabilités connues affectent ce système.

- CPE (Common Platform Enumeration) :

o La ligne cpe:/o:linux:linux_kernel indique qu'il s'agit d'un noyau Linux générique.

Recommandations :

1. Mettre à jour le système :

o Mettez à jour Debian vers une version supportée (comme Debian 11 ou 12).

o Mettez à jour OpenSSH (version récente comme 9.x) et Apache (version 2.4.x).

2. Restreindre l'accès SSH :

o Limitez les connexions SSH aux IP spécifiques.

o Désactivez l'authentification par mot de passe et utilisez des clés SSH.

o Utilisez des outils comme Fail2Ban pour prévenir les tentatives de brute force.

3. Sécuriser le serveur HTTP :

o Appliquez des correctifs de sécurité si une mise à jour n'est pas immédiatement possible.

o Désactivez les modules inutiles et limitez l'accès aux fichiers sensibles.

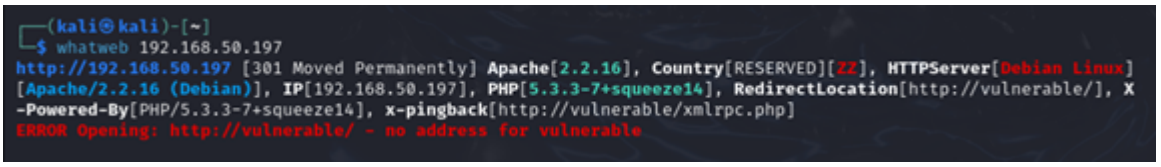
4. Analyse des vulnérabilités :

o Effectuez un audit complet avec des outils comme Nessus, OpenVAS, ou Metasploit pour vérifier les exploits applicables.

5. Isolation réseau :

o Si possible, limitez l'accès à ce serveur uniquement à partir du réseau local ou via un VPN.

- Analyse des technologies utilisées : serveur web, plugins WordPress, bibliothèques tierces.



1. Statut HTTP : 301 (Moved Permanently)

- Description : Le serveur renvoie une redirection permanente (code HTTP 301) vers une nouvelle URL : http://vulnerable/.
- Problème : L'URL http://vulnerable/ ne peut pas être résolue en une adresse IP valide, probablement parce qu'il manque une configuration DNS ou un hôte local pour "vulnerable".

---

2. Serveur Web

- Logiciel utilisé : Apache 2.2.16
  - Hébergé sur Debian Linux (distribution obsolète, "Squeeze").
  - Problème : Apache 2.2.16 est une version ancienne (sortie en 2010) contenant des vulnérabilités connues :
    - CVE-2011-3192 : Attaque par déni de service (DoS).
    - CVE-2012-0053 : Vulnérabilités dans la gestion des requêtes.
  - Les mises à jour ne sont plus disponibles pour cette version.

---

3. PHP (Version 5.3.3-7+squeeze14)

- Description : Le serveur exécute PHP pour le traitement de contenu dynamique.
- Version obsolète : PHP 5.3.3 est également très ancien et n'est plus pris en charge depuis 2014. Cette version est vulnérable à des attaques telles que :
  - Exécution de code à distance (RCE).
  - Injection SQL via des requêtes mal protégées.
  - Failles dans les fonctions serialize() et unserialize().

---

4. Redirection et x-pingback

- Redirection : RedirectLocation[http://vulnerable/]

o Le serveur redirige les requêtes vers l'URL http://vulnerable/. Cependant, cette URL n'est pas valide car elle n'est pas résolue en adresse IP.

o Cela peut indiquer :

Une configuration erronée ou incomplète du serveur.

Un environnement de test mal configuré.

- x-pingback : x-pingback[http://vulnerable/xmlrpc.php]

o Cette en-tête HTTP indique que le fichier xmlrpc.php est activé. Ce fichier est couramment utilisé pour des fonctionnalités entre sites (comme les pingbacks).

o Problème : XML-RPC est une cible d'attaque fréquente. Les risques incluent :

Amplification des attaques DDoS.

Brute force pour compromettre les identifiants.

Injections XML.

---

5. Adresse IP

- 192.168.50.197 : Adresse IP privée utilisée dans un réseau local. Elle ne correspond à aucun pays (Country[RESERVED][ZZ]) car elle est réservée pour des usages internes.

---

6. Erreur de résolution DNS

- Message d'erreur : ERROR Opening: http://vulnerable/ - no address for vulnerable

o Cette erreur signifie que le domaine "vulnerable" ne peut pas être résolu en une adresse IP.

o Cela est souvent dû à :

L'absence d'une configuration DNS locale.

Une redirection incorrecte ou incomplète sur le serveur.

Problèmes identifiés :

1. Vulnérabilités dues à des versions obsolètes :
    - Apache 2.2.16.
    - PHP 5.3.3.
    - Debian Squeeze.
2. Configuration erronée de la redirection vers "vulnerable".
3. Exposition de fonctionnalités risquées comme xmlrpc.php.

Recommandations :

1. Mettre à jour :
    - Mettez à jour le serveur avec une version récente de Debian et des logiciels utilisés (Apache 2.4.x, PHP 8.x).
    - Supprimez ou désactivez les fonctionnalités inutiles comme xmlrpc.php.
2. Corriger la redirection :
    - Assurez-vous que l'URL cible http://vulnerable/ pointe vers une ressource valide et accessible.
3. Sécuriser le serveur :
    - Appliquez des correctifs de sécurité.
    - Activez des mécanismes de défense comme un pare-feu (iptables, UFW) pour limiter les accès.

- Collecte d'informations publiques (OSINT) pour détecter des informations sensibles exposées.

L'OSINT (Open Source Intelligence) désigne la collecte et l'analyse d'informations disponibles publiquement pour en extraire des renseignements exploitables. Ces informations peuvent provenir de sources variées telles que des réseaux sociaux, des forums, des sites d'entreprise, des bases de données publiques ou encore des médias traditionnels.

L'OSINT est une composante clé dans de nombreux domaines, notamment la cybersécurité, les enquêtes criminelles et le renseignement économique. Dans le cadre de la cybersécurité, il permet par exemple d'identifier les vulnérabilités exposées publiquement, les fuites de données sensibles ou encore les configurations à risque.

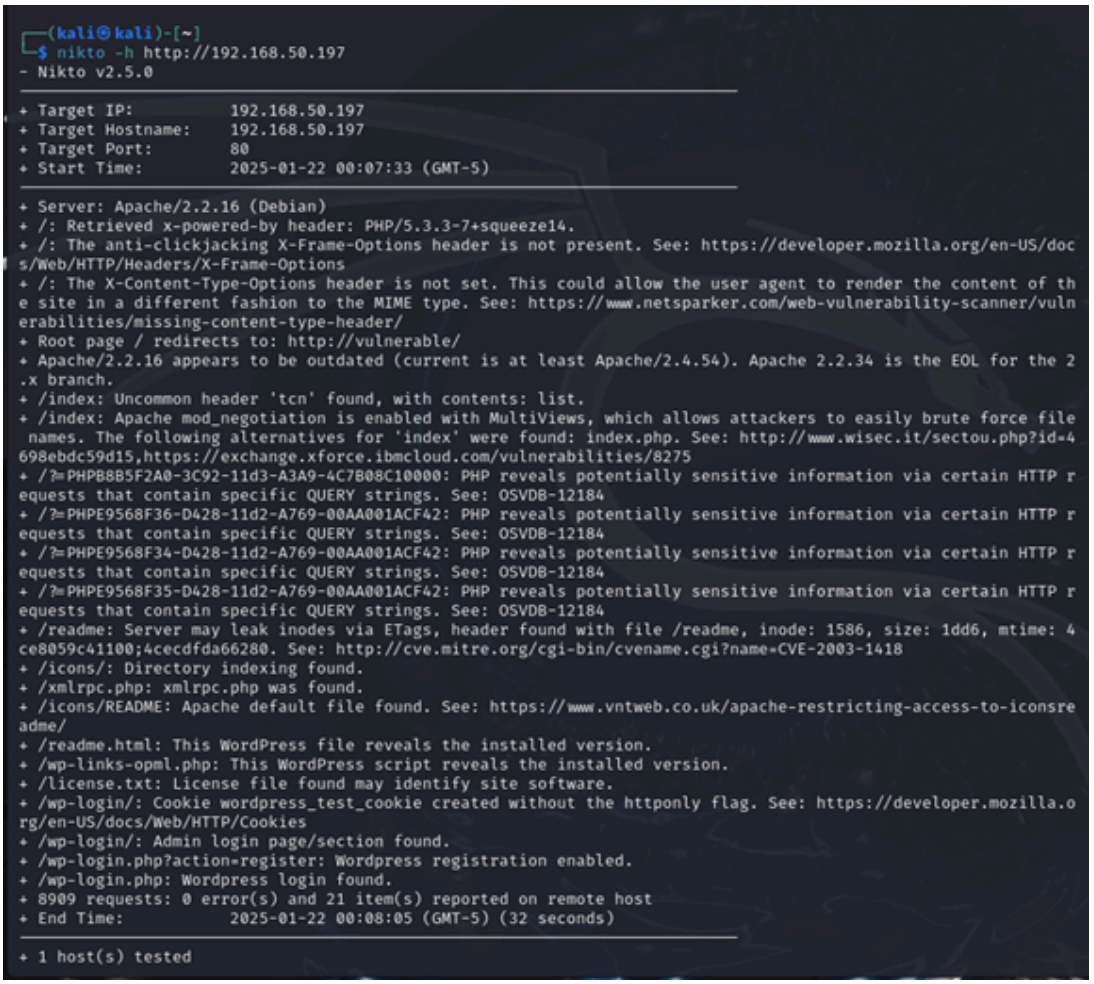
Bien que l'OSINT soit souvent sous-estimé, il peut jouer un rôle déterminant dans la sécurisation des systèmes et la protection des données d'une entreprise. C'est pourquoi il est essentiel de le mentionner, même si ce point n'a pas été traité en détail ici. Une démarche proactive dans ce domaine permet non seulement de mieux se protéger contre les cybermenaces mais aussi d'anticiper d'éventuelles attaques.

3. Analyse des vulnérabilités :

- Utilisation de WPScan pour lister les vulnérabilités propres à l'écosystème WordPress.

- Comparaison avec les CVE disponibles pour vérifier si le site est affecté par des vulnérabilités connues, notamment CVE-2008-1930.

- Inspection manuelle du code source accessible pour repérer des failles potentielles.



1. Informations générales

- Serveur web : Apache/2.2.16 (Debian).
- PHP : 5.3.3-7+squeeze14.
- Redirection : La page principale (/) redirige vers http://vulnerable/.

Ces versions obsolètes présentent des vulnérabilités connues et ne sont plus maintenues. Cela expose le serveur à des attaques potentielles.

---

2. En-têtes HTTP manquants

- X-Frame-Options :

o Non présent.

o Risque : Vulnérabilité aux attaques de type clickjacking (les utilisateurs peuvent être trompés pour interagir avec des interfaces malveillantes invisibles).

o Solution : Ajouter X-Frame-Options: SAMEORIGIN ou DENY dans les configurations.

- X-Content-Type-Options :

o Non présent.

o Risque : Permet le MIME sniffing, où le navigateur interprète incorrectement les types de fichiers (risque de téléchargement malveillant).

o Solution : Ajouter X-Content-Type-Options: nosniff.

---

3. Vulnérabilités dans PHP

- Les requêtes avec des paramètres spécifiques (?=PHP...) révèlent des informations sensibles :

o Risque : Ces paramètres spéciaux affichent des informations sur PHP et sa configuration (comme le logo PHP, les crédits). Cela facilite la reconnaissance par des attaquants.

o Solution : Désactiver l'exposition d'informations dans le fichier php.ini en configurant :

Le message d'erreur que vous avez obtenu avec sslscan indique que la connexion au port 443 (qui est généralement utilisé pour HTTPS) a été refusée. Cela signifie que le serveur ne répond pas sur ce port ou qu'il n'a pas de service HTTPS (SSL/TLS) actif à l'adresse 192.168.50.197.

Voici quelques raisons pour lesquelles cela pourrait se produire :

1. HTTPS désactivé : Le serveur ne dispose pas d'un service HTTPS ou SSL configuré, et donc le port 443 est fermé.

2. Pare-feu ou filtre réseau : Un pare-feu ou une règle de filtrage pourrait bloquer l'accès au port 443.

3. Serveur mal configuré : Il est possible que le serveur n'ait pas correctement configuré ou activé SSL/TLS pour le port 443.

4. Service non démarré : Si le service HTTPS est en cours de démarrage ou est désactivé pour d'autres raisons, il peut être temporairement inaccessible.

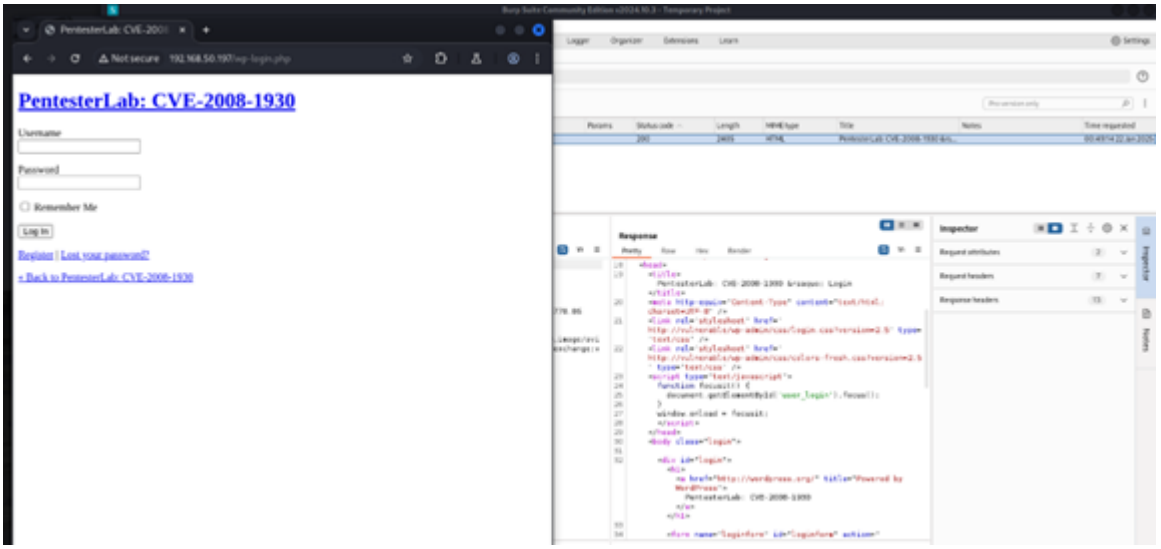
Étapes pour vérifier et corriger :

1. Vérifier la configuration du serveur Apache : Si le serveur utilise Apache, assurez-vous qu'il est configuré pour accepter les connexions HTTPS. Vérifiez la présence d'un fichier de configuration pour HTTPS, souvent appelé ssl.conf ou une entrée pour le port 443 dans les fichiers de configuration d'Apache (comme 000-default.conf ou default-ssl.conf).

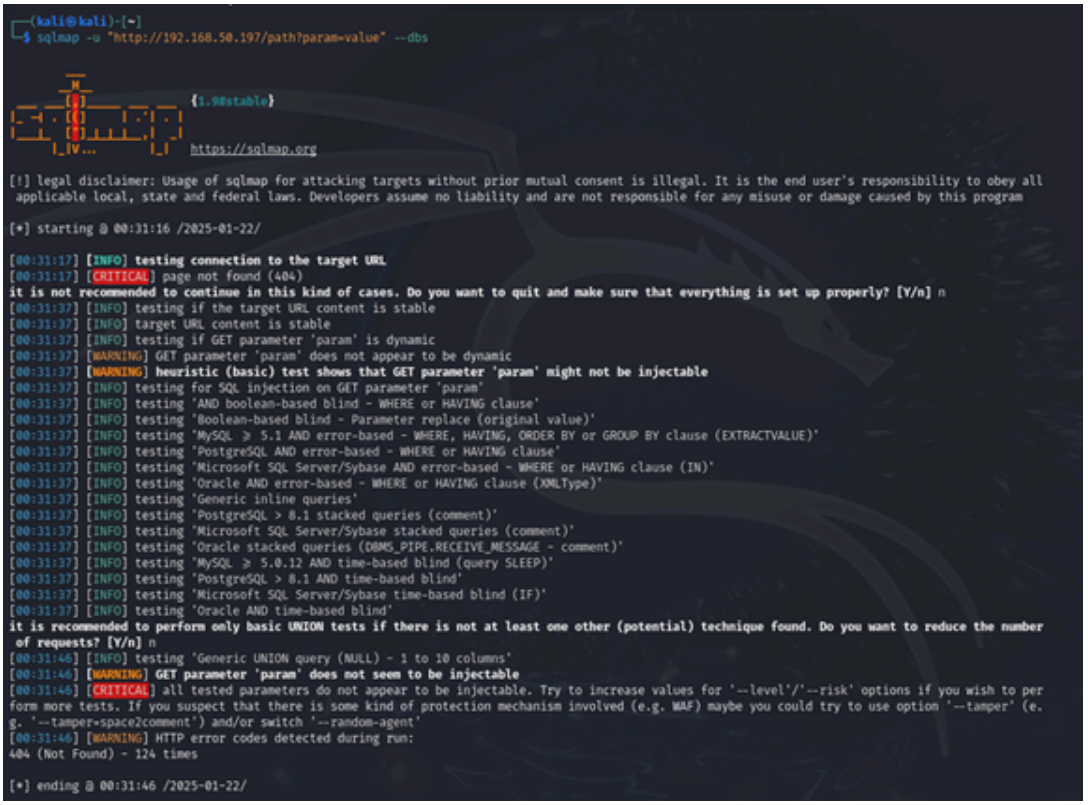
2. Vérifier le pare-feu : Assurez-vous qu'aucun pare-feu (sur le serveur ou sur le réseau) n'empêche les connexions entrantes sur le port 443. Vous pouvez vérifier cela en utilisant des outils comme ufw (pour Ubuntu/Debian) ou firewalld (pour d'autres distributions).

4. Exploitation :

- Validation des vulnérabilités par des tests d'exploitation limités utilisant des outils comme Metasploit ou Burp Suite.

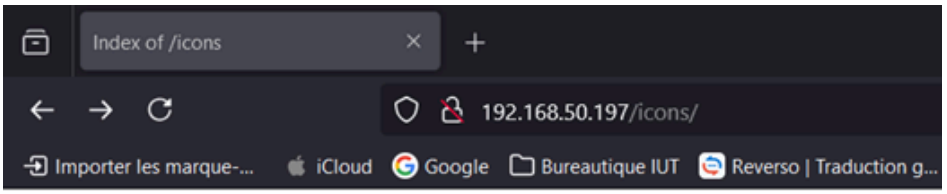


- Cette capture montre la page de connexion WordPress du laboratoire PentesterLab: CVE-2008-1930.
- L'URL 192.168.50.197/wp-login.php indique un serveur local vulnérable.
- L'absence de HTTPS (indiqué par "Not secure") montre que les données d'authentification sont envoyées en clair, facilitant leur interception via Man-in-the-Middle (MITM).
- Burp Suite est utilisé pour capturer et analyser les requêtes HTTP envoyées à WordPress.



- SQLMap n'a pas trouvé de vulnérabilité SQL Injection sur l'URL testée.
- L'échec peut être dû à **une protection WAF, une page inexistante ou une sécurisation correcte du paramètre**.
- D'autres méthodes (scan des paramètres, bypass WAF) peuvent être tentées pour approfondir l'analyse.

Exploitation de la sortie de la commande nikto

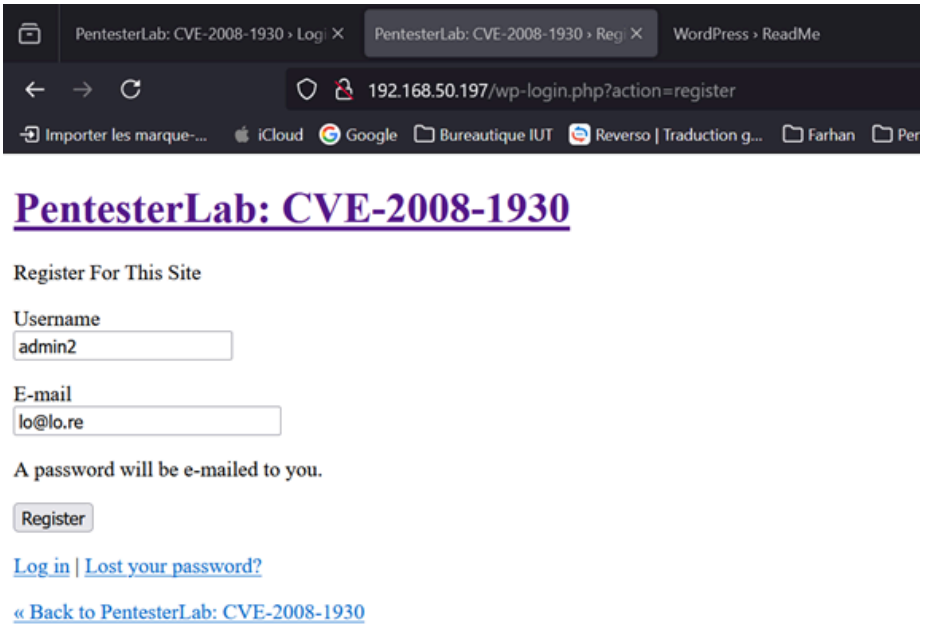


Index of /icons

Name	Last modified	Size	Description
Parent Directory		-	
README	28-Aug-2007 10:48	5.0K	
README.html	28-Aug-2007 10:48	35K	
a.gif	20-Nov-2004 20:16	246	
a.png	26-Nov-2008 06:36	306	
alert.black.gif	20-Nov-2004 20:16	242	
alert.black.png	26-Nov-2008 06:36	293	
alert.red.gif	20-Nov-2004 20:16	247	
alert.red.png	26-Nov-2008 06:36	314	
apache_pb.gif	20-Nov-2004 20:16	2.3K	
apache_pb.png	26-Nov-2008 06:36	2.0K	
apache_pb2.gif	26-Nov-2008 06:36	1.8K	
apache_pb2.png	26-Nov-2008 06:36	1.5K	
apache_pb2_ani.gif	26-Nov-2008 06:36	2.4K	
back.gif	20-Nov-2004 20:16	216	
back.png	26-Nov-2008 06:36	308	
ball.gray.gif	20-Nov-2004 20:16	233	

- **Indexation activée** : Le serveur Apache autorise l'affichage du contenu du dossier `/icons/`, révélant tous les fichiers qu'il contient.
- **Fuite d'informations** : Des fichiers comme `README.html` peuvent contenir des détails sensibles sur la configuration du serveur.
- **Identification du serveur** : La présence de fichiers `apache_pb.gif` indique que le serveur utilise **Apache**, aidant un attaquant à adapter ses attaques.
- **Potentiel d'exploitation** : Un attaquant peut rechercher des fichiers oubliés (`backup`, `.bak`, `config.php`) pouvant contenir des données critiques.
- **Configuration incorrecte d'Apache** : L'activation de l'indexation (`Indexes`) est une faille de sécurité qui doit être corrigée.

- **Solution** : Désactiver l'indexation en ajoutant `Options -Indexes` dans la configuration Apache ou `.htaccess`, et restreindre l'accès aux fichiers sensibles.



- Cette capture illustre la page d'inscription WordPress (`wp-login.php?action=register`).
- L'utilisateur "admin2" est en train d'être créé.
- Si l'auto-inscription avec des privilèges élevés est activée, cela représente une faille de configuration critique.

Nous allons exploiter la faille de vulnérabilité :

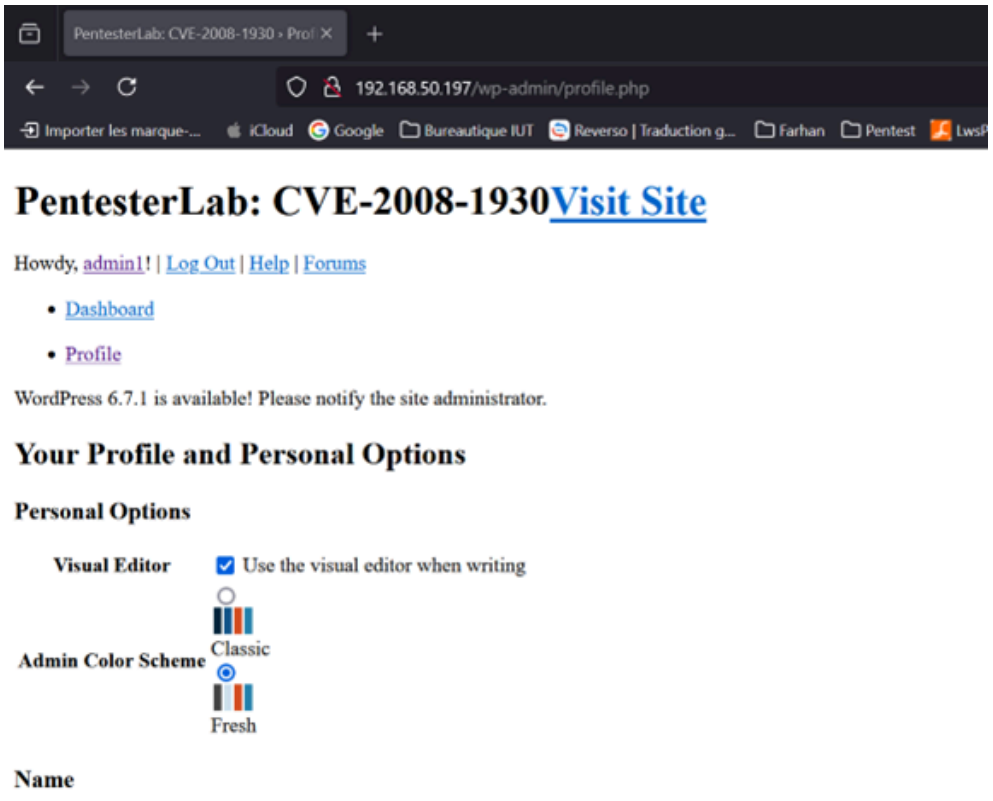
Cette vulnérabilité découverte en 2008 concerne une faille dans le mécanisme d'intégrité des cookies de WordPress. Elle permet à un attaquant de devenir administrateur du site si l'enregistrement des utilisateurs est activé. L'attaque repose sur une faiblesse cryptographique liée à une collision de hachage dans la fonction de validation des cookies.

Lorsqu'un utilisateur se connecte, WordPress génère un cookie `AUTH_COOKIE` contenant trois informations :

- **Nom d'utilisateur (`$username`)**
- **Date d'expiration (`$expiration`)**
- **HMAC (hash signé pour vérifier l'intégrité)**

La validation du cookie utilise une fonction de hachage `hash_hmac('md5', $username . $expiration, $key)`.

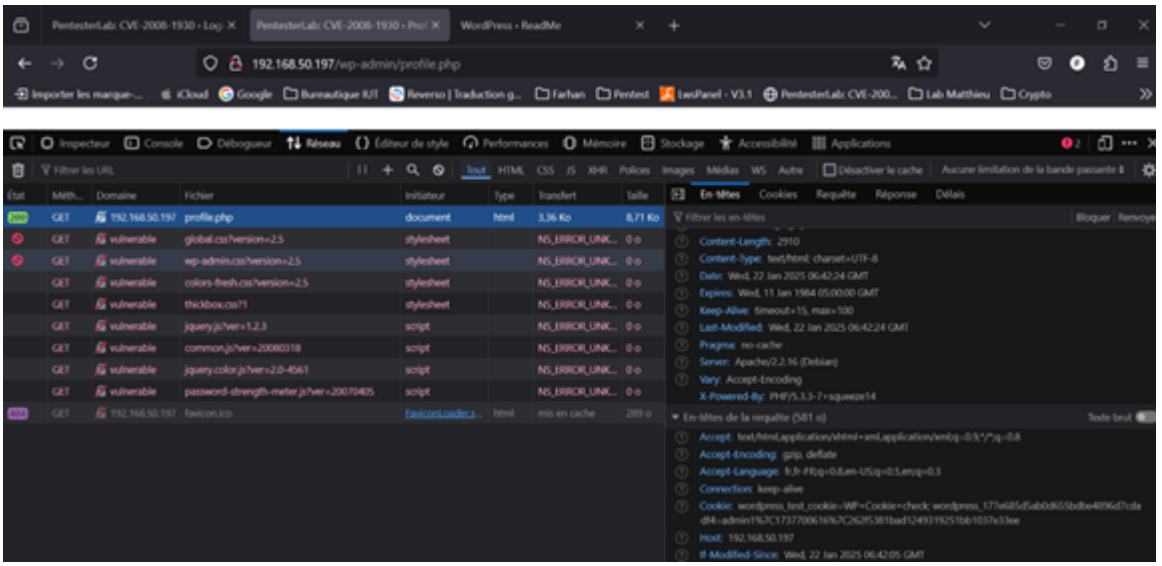
Nous avons pu créer un nouvel utilisateur avec la fonction Register.



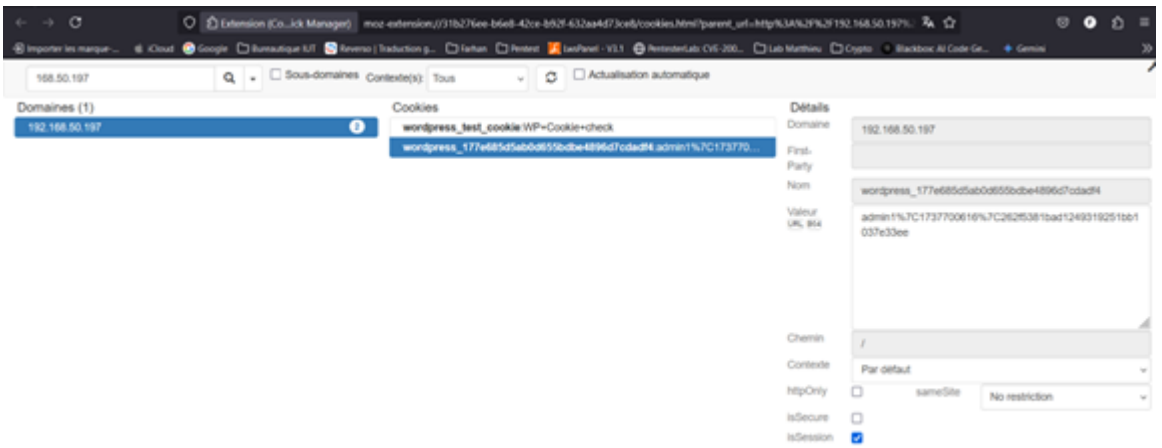
- La validation du cookie utilise une fonction de hachage `hash_hmac('md5', $username . $expiration, $key)`.
- Problème : il est possible de générer une collision de hachage entre deux paires différentes de `$username` et `$expiration`.

Cette collision permet à un attaquant ayant un compte utilisateur `admin1` d'obtenir un cookie valide pouvant être modifié pour prétendre être `admin`.

L'attaquant s'enregistre avec un nom d'utilisateur suivi d'un chiffre, par exemple `admin1`.



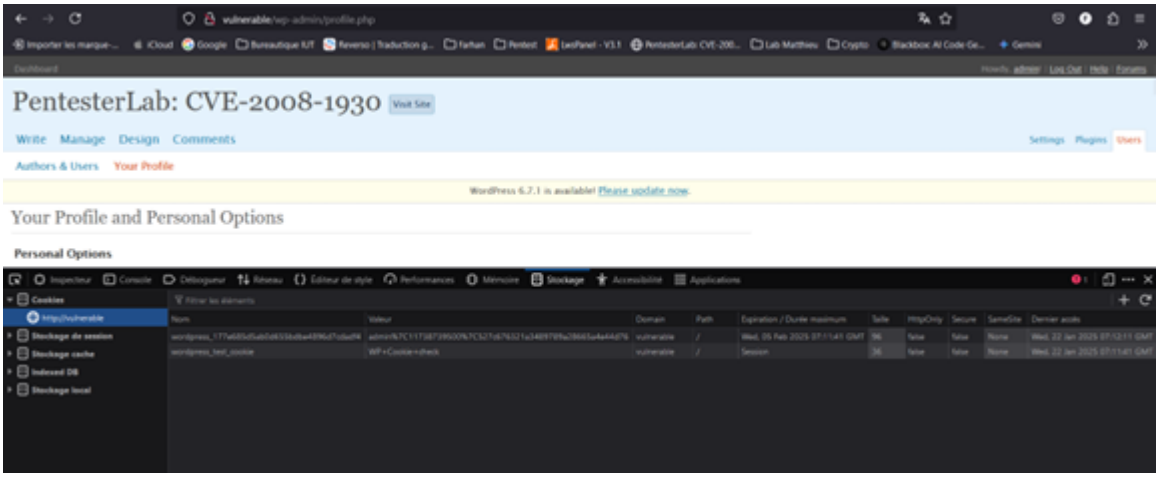
Après connexion, le cookie suivant est généré :



L'attaquant remplace `admin1` par `admin` et ajuste l'expiration pour obtenir :

admin%7C11210158445%7C49718d2581bd399916b90a088a11ec84

En rechargeant la page avec ce cookie modifié, l'attaquant accède à la version admin du site.



5. Post-exploitation :

- Évaluation des données compromises (fichiers de configuration, bases de données sensibles).

- Analyse de la possibilité de maintenir un accès persistant au système.

2.2 Outils Utilisés

- Nmap : Scan de ports et services.
- WPScan : Analyse des vulnérabilités spécifiques à WordPress.
- Burp Suite : Interception et modification de requêtes HTTP pour tester des failles logiques.
- Metasploit : Exploitation automatisée des vulnérabilités connues.
- Nikto : Scan de vulnérabilités pour les serveurs web.

6. Résultats de l'Audit

6.1 Vulnérabilités Identifiées

- **Version vulnérable de WordPress détectée** : Version < 2.5.1.
- **Exploitation réussie** : Accès administrateur obtenu via la manipulation des cookies.
- **Données sensibles accessibles** : Fichiers de configuration, base de données.
- **Risque majeur** : Possibilité de détournement du site et vol de données utilisateurs.

7. Recommandations et Plan d'Action

7.1 Recommandations :

- Mettre à jour WordPress vers la version la plus récente.
- Forcer l'utilisation de cookies HTTPOnly et Secure pour empêcher les manipulations.
- Régénérer les clés de session pour invalider les cookies compromis.
- Restreindre l'accès à l'interface d'administration via un filtrage IP.
- Activer l'authentification à double facteur pour renforcer la sécurité des comptes admin.

7.2 Plan d'Actions

Action	Priorité	Responsable	Délai
Mise à jour de WordPress	Haute	Administrateur web	Immédiate
Activation HTTPS et cookies sécurisés	Haute	Administrateur système	1 semaine
Implémentation de l'authentification à deux facteurs	Moyenne	Responsable sécurité	2 semaines
Audit périodique des sessions et des logs	Moyenne	Équipe de sécurité	Mensuel

8. Conclusion de l'audit

L'audit a permis d'identifier et d'exploiter la vulnérabilité **CVE-2008-1930**, mettant en évidence des failles critiques dans la gestion des cookies d'authentification de WordPress. L'exploitation de cette vulnérabilité peut avoir des conséquences graves, telles que la compromission des comptes administrateurs et l'exfiltration de données sensibles.

L'application des recommandations et du plan d'actions définis permettra de réduire considérablement ces risques et d'assurer une meilleure sécurité de la plateforme.

Conclusion

Le projet **SAE 5.CYBER 3 - Assurer la sécurisation et la supervision avancée d'un système d'information** a permis de concevoir et de déployer une infrastructure sécurisée et segmentée, répondant aux exigences de protection des systèmes critiques.

Objectifs atteints

- Mise en place d'un **SOC** avec une supervision centralisée grâce à **Wazuh, Zabbix et Grafana**.
- Détection proactive des menaces via **CrowdSec et les IDS/IPS d'OPNsense**.
- Sécurisation des services internes avec **Active Directory et des politiques GPO adaptées**.
- Implémentation de **contrôles stricts d'authentification et de segmentation réseau**.
- Protection des applications exposées grâce à un **proxy inversé** et un **pare-feu applicatif (WAF)**.
- Mise en place de connexions **HTTPS chiffrées** pour garantir l'intégrité des données.
- Réalisation d'un **audit de sécurité approfondi**, incluant l'évaluation de la posture Active Directory avec **PingCastle**, l'exploitation de vulnérabilités WordPress (CVE-2008-1930) et l'application de correctifs pour renforcer la sécurité.

Résultats obtenus

- **Sécurité renforcée** par une segmentation stricte des zones réseau et une gestion fine des accès via **Teleport** et une authentification multi-facteurs.
- **Supervision avancée** avec une surveillance en temps réel des performances et des incidents de sécurité.
- **Conformité aux normes de cybersécurité** en intégrant des recommandations de l'ANSSI et des principes ISO/IEC 27001.
- **Amélioration continue** grâce à des audits réguliers et des mises à jour des politiques de sécurité.

Perspectives et évolutions futures

- **Renforcement des défenses** par l'intégration d'outils de détection et de réponse aux menaces tels que **EDR** et **SOAR**.
- **Optimisation de la supervision** avec des tests d'intrusion réguliers et une gestion plus efficace des journaux et des alertes.
- **Formation et sensibilisation des utilisateurs** pour limiter les risques liés aux erreurs humaines et améliorer la posture de cybersécurité.

Annexes

Annexes : Configurations détaillées

1. Topologie Réseau et Adresses IP

Zone	Équipement	Adresse IP	Description
Pare-feu	OPNsense (WAN)	10.81.1.x/24	Connecté au réseau externe (Réseau de simulation)
	OPNsense (LAN)	192,168.1.1/24	Point de routage vers les VLAN internes
	OPNsense (em2)	10.81.150.1/24	Connexion au bastion
Zone SOC	Wazuh-Indexer	10.81.110.60/24	Serveur d'indexation des journaux
	Wazuh-Dashboard	10.81.110.50/24	Interface utilisateur
	Wazuh-Manager	10.81.110.70/24	Gestion des agents et corrélation
	Zabbix	10.81.110.110/24	Plateforme de supervision réseau
	BDD (Zabbix)	10.81.110.120/24	Base de données dédiée
	Deming	10.81.110.80/24	Évaluation et reporting des mesures de sécurité
	Mercator	10.81.110.90/24	Cartographie des systèmes d'information
Zone Services	Active Directory	10.81.120.10/24	Gestion des identités et des accès
	SRV-Stockage	10.81.120.11/24	Serveur de stockage sécurisé
	Grafana	10.81.120.20/24	Visualisation des données réseau et système
Zone Front	webterm-1 (Docker)	DHCP	Application web conteneurisée
	Windows10-1	DHCP	Poste de travail pour tests
	webserver-1	10.81.130.50/24	Serveur applicatif exposé
Bastion	Teleport Bastion	10.81.140,50/24	Point d'accès sécurisé pour les administrateurs

2. Configurations détaillées

2.1. Pare-feu (OPNsense)

A. Interfaces OPNsense

- **WAN** :
  - Adresse IP : 10.81.1.x/24 (Externe).
  - Connecté au réseau externe pour gérer les connexions entrantes.
- **LAN** :
  - Adresse IP : 192.168.1.1/24.
  - Point de routage pour les VLAN internes, connectant les zones SOC, Services et Front.
- **INTERCO** :
  - Adresse IP : 10.81.150.1/24.
  - Connexion dédiée au bastion Teleport pour les accès administratifs sécurisés.
- **ADMIN** :
  - Adresse IP : 10.81.255.1/24.
  - Réseau administratif entièrement séparé des autres VLANs.

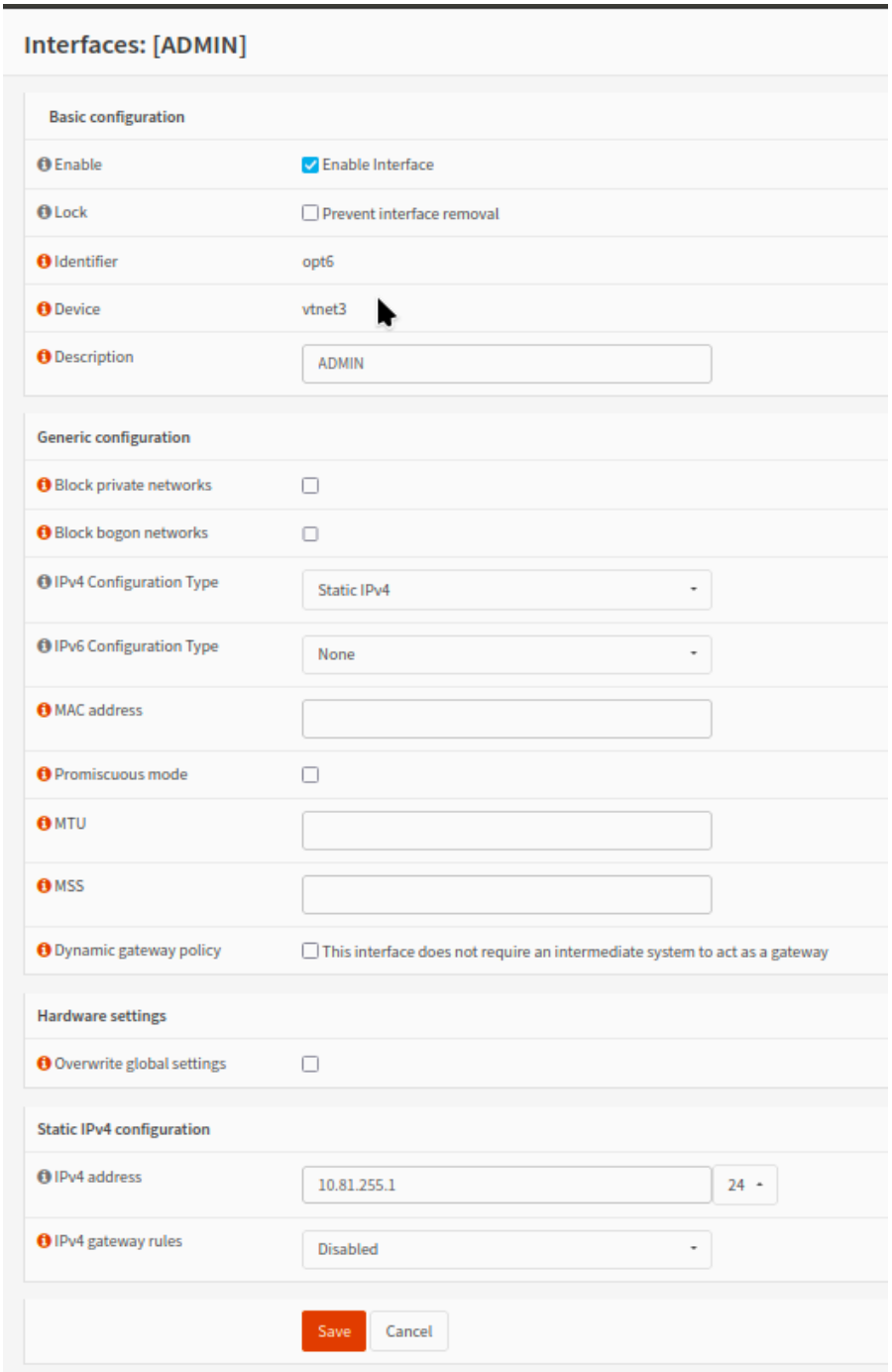
B. Règles de Pare-feu

- **WAN → Zone Front** :
  - Autorisé uniquement pour les protocoles HTTP/HTTPS vers le serveur webserver-1.
- **Zone SOC → Zone Services** :
  - Communication autorisée pour les outils de supervision tels que Zabbix et Grafana.
- **Zone Front → Zone SOC** :
  - Interdit, sauf pour webterm-1 (pour l'envoi de journaux vers le SOC).
- **Bastion → Zones SOC, Services et Front** :
  - Autorisé uniquement pour les protocoles SSH et les opérations administratives.

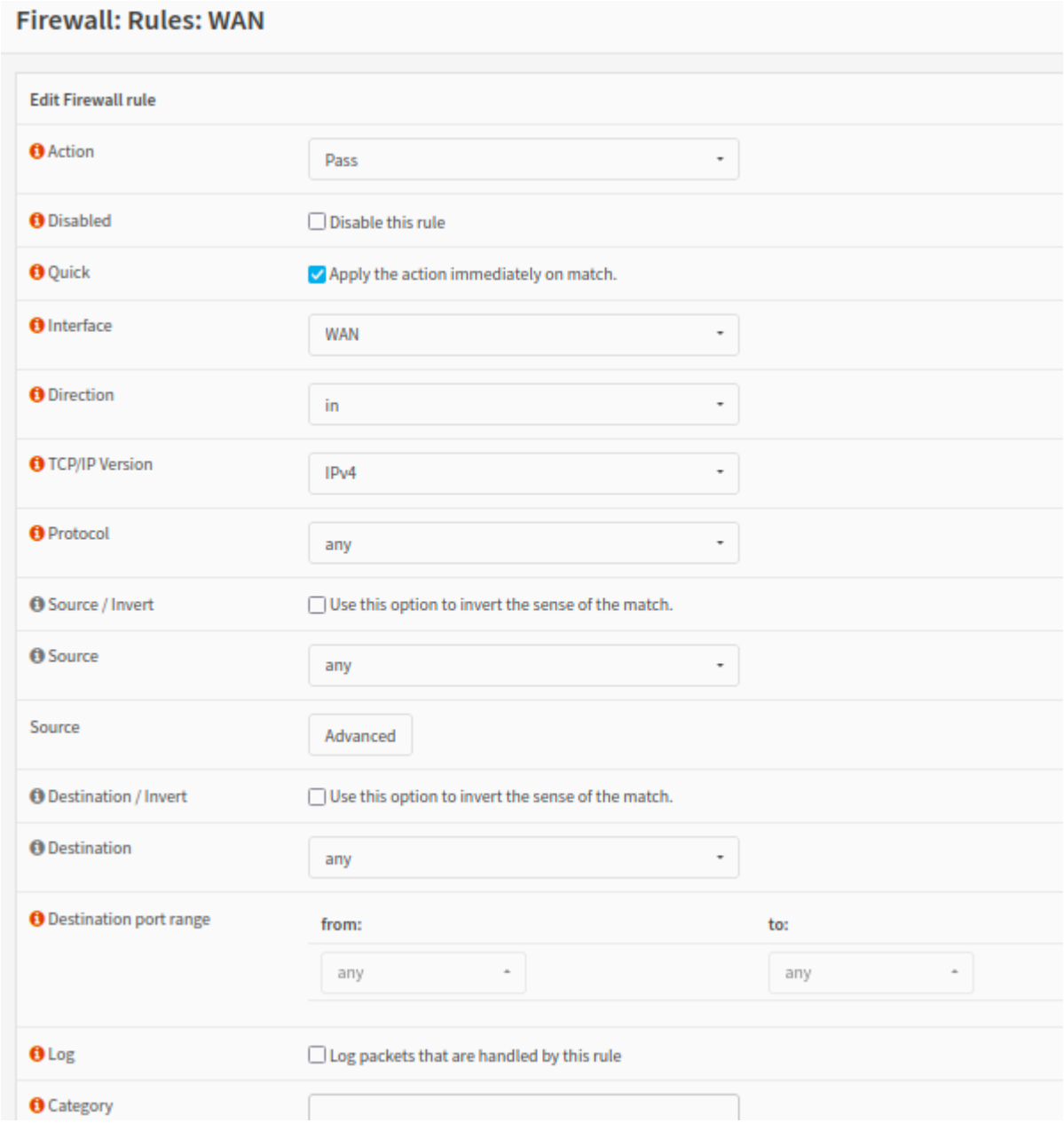
c. DHCP

- Les VLAN internes sont configurés avec une attribution statique des adresses IP pour garantir une gestion réseau précise et éviter les conflits d'adresses.

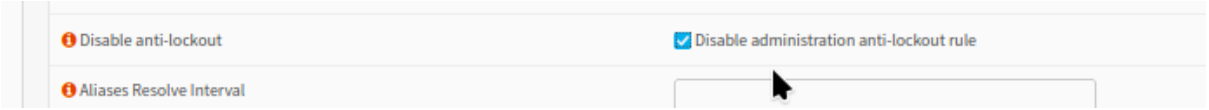
Configuration de 10.81.255.1/24 comme étant le réseau de l'interface Admin :



Puis sauvegarder et aller dans la section Firewall > Règles > WAN et ajouter une règle qui autorise tout pour les administrateurs:



Puis aller dans Firewall > Réglages > Avancé et cocher “Disable anti-lockout”



2.2. Switch

- **VLANs configurés :**
  - VLAN 10 : Zone SOC (10.81.110.0/24)
  - VLAN 20 : Zone Services (10.81.120.0/24)
  - VLAN 30 : Zone Front (10.81.130.0/24)
  - VLAN 40 : Zone Bastion (10.81.140.0/24)
- **Trunk :**
  - Trunk configuré entre le switch et OPNsense pour permettre la segmentation VLAN.
- **Ports assignés :**
  - Ports spécifiques pour chaque VLAN (exemple : VLAN 110 pour SOC sur ports 1-5).

2.3. Zone SOC

- **Wazuh (Indexer, Dashboard, Manager) :**
  - **Configuration locale :**
    - Logs collectés des agents connectés.
    - Tableau de bord configuré pour afficher les alertes critiques.
  - **Agent CrowdSec :**
    - Connecté à la LAPI d'OPNsense.
- **Zabbix :**
  - Supervision active des équipements réseau, métriques CPU/RAM/Stockage.
  - Base de données sécurisée avec sauvegarde automatique.

2.4. Zone Services

- **Active Directory (Windows Server) :**
  - GPO renforcées pour les mots de passe et comptes inactifs.
  - MFA activé pour tous les utilisateurs.
- **SRV-Stockage :**
  - Chiffrement activé pour les données partagées.
  - Sauvegardes régulières vers un NAS sécurisé.
- **Grafana :**
  - Dashboards configurés pour surveiller Wazuh, CrowdSec, et Zabbix.
  - Alertes paramétrées pour dépassements de seuils critiques.

2.5. Zone Front

- **webterm-1 :**
  - Conteneur Docker sécurisé avec isolation stricte.
  - Services accessibles uniquement via HTTPS.
- **webserver-1 :**
  - Protégé par un WAF pour bloquer les attaques web (Injection SQL, XSS).
  - Trafic filtré par le proxy inversé.
- **Proxy inversé :**
  - Redirige les requêtes autorisées vers les services Front.
  - Bloque les requêtes suspectes.

3. DHCP Configuration

- **Plages IP réservées par VLAN :**
  - VLAN 10 : 10.81.110.10 - 10.81.110.100
  - VLAN 20 : 10.81.120.10 - 10.81.120.100
  - VLAN 30 : 10.81.130.10 - 10.81.130.100
  - VLAN 40 : 10.81.140.10 - 10.81.140.100
- **Options DHCP :**
  - Gateway : 10.81.1xx.1 (selon le VLAN)
  - DNS : Configuré pour rediriger vers les serveurs internes et externes.

Annexe : Tableau des flux réseau entre les serveurs

Le tableau ci-dessous détaille les flux réseau autorisés entre les différents serveurs et équipements décrits dans la topologie.

Source	Destination	Protocole	Port(s)	Description
Teleport Bastion	Tous les serveurs	SSH/TLS	22, 443,80	Connexion sécurisée centralisée pour l'administration.
Wazuh-Agent (ex. Deming, Mercator)	Wazuh-Manager	HTTPS, TCP	1514, 443	Envoi des logs et des métriques pour supervision.
Wazuh-Manager	Wazuh-Dashboard	HTTP/HTTPS	443	Communication entre le backend et l'interface utilisateur.
Wazuh-Manager	Wazuh-Indexer	HTTP/HTTPS	9200	Indexation et stockage des journaux collectés.
Grafana	Zabbix	HTTP/HTTPS	80, 443	Collecte des données de supervision pour affichage.
Webterm-1	Web Server (webserver-1)	HTTP/HTTPS	80, 443	Accès aux applications web hébergées sur le serveur frontal.
Windows10-1/2	Teleport Bastion	RDP/SSH	3389, 22	Connexions distantes via le bastion.
Tous les serveurs Windows	Active Directory	LDAP/Kerberos	389, 636, 88	Authentification et gestion des identités.
SRV-Stockage	Tous les serveurs	SMB/NFS	445, 2049	Partage et stockage sécurisé des fichiers.
Firewall (OPNsense)	Internet (WAN)	NAT	80, 443, autres	Accès aux ressources externes via NAT (web, mises à jour, etc.).
Wazuh-Manager	Zabbix	TCP	10050, 10051	Intégration pour la supervision avancée des agents.

Notes :

- **Filtrage des flux** : Tous les flux sont configurés pour limiter les communications au strict nécessaire, renforçant la sécurité.
- **Centralisation** : Les connexions administratives passent exclusivement par le bastion Teleport.
- **Supervision** : Les communications entre les composants de Wazuh et ses agents assurent la collecte, le traitement et l'affichage des données pour la supervision.

Règles sur le pare-feu:

Source	Destination	Protocole	Port(s)	Description
BASTION, FRONT, SERVICE, SOC	Active Directory	TCP/UDP	389 (LDAP), 53 (DNS), 445 (MS DS), 135, 636, 88	Ports nécessaires pour l'active directory
BASTION, FRONT, SERVICE, SOC	BASTION	TCP	443	Connexion des hôtes pour les agents Teleport
BASTION, FRONT, SERVICE, SOC	Wazuh-Manager	TCP	1515	Accès des agents Wazuh au Wazuh Manager
BASTION, FRONT, SERVICE, SOC	Wazuh-Manager	TCP	1514	Accès des agents Wazuh au Wazuh Manager.
BASTION, FRONT, SERVICE, SOC	Wazuh-Manager	TCP	55000	Accès à l'api RESTful de Wazuh
BASTION, FRONT, SERVICE, SOC	Zabbix	TCP/UDP	10051	Accès vers le collecteur Zabbix pour les agents
BASTION, FRONT, SERVICE, SOC	Firewall	TCP	8080	Utilisé par CrowdSec
ADMIN	any	any	any	Accès du réseau admin à tout
BASTION	FRONT, SERVICE, SOC	TCP	22 (SSH), 80 (HTTP), 443 (HTTPS)	Autoriser le bastion à se connecter
SERVICE	10.81.110.110	TCP	80 (HTTP)	Connexion de

	(Zabbix)			Grafana à l'api Zabbix
SOC	10.81.255.1/24 10.81.140.1/24 10.81.130.1/24 10.81.150.1/24 10.81.120.1/24 10.81.110.1/24	TCP/UDP	10050	Connexion de Zabbix à ses agents pour le polling

Annexe : Détails d'installation de Teleport et de ses agents

1. Installation de Teleport sur le Bastion

Prérequis :

1. **Système d'exploitation :**
    - Ubuntu 22.04 ou CentOS 8 recommandé.
2. **Accès administrateur :**
    - Utilisateur avec des privilèges sudo.
3. **Ressources réseau :**
    - Ports ouverts :
        - **443** (HTTPS) pour le proxy.
        - **3022-3025** pour les services Teleport (SSH, RDP, API).
4. **Certificat TLS :**
    - Certificat valide ou auto-signé pour sécuriser les connexions HTTPS.

Étapes d'installation :

1. **Télécharger et installer Teleport :**

Téléchargez la version la plus récente depuis le site officiel de Teleport :

```
sudo curl https://goteleport.com/static/install.sh | bash -s
17.1.1
```

Configurer le fichier `teleport.yaml` :

```
nano /etc/teleport.yaml
```

```
version: v3
teleport:
  nodename: debian
  data_dir: /var/lib/teleport
  log:
    output: stderr
    severity: INFO
    format:
      output: text
  ca_pin: ""
  diag_addr: ""
auth_service:
  enabled: "yes"
  listen_addr: 0.0.0.0:3025
  cluster_name: teleport.gns3.lab.mpgn.dev
  proxy_listener_mode: multiplex
ssh_service:
  enabled: "yes"
  commands:
  - name: hostname
    command: [hostname]
    period: 1m0s
```

```
proxy_service:
  enabled: "yes"
  web_listen_addr: 0.0.0.0:443
  public_addr: teleport.gns3.lab.mpgn.dev:443
  https_keypairs:
    - cert_file: /var/lib/teleport/fullchain.pem
      key_file: /var/lib/teleport/privkey.pem
  https_keypairs_reload_interval: 0s
  acme: {}
```

2. **Démarrer le service Teleport :**

```
sudo systemctl daemon-reload
sudo systemctl enable teleport
sudo systemctl start teleport
```

3. **Configurer un administrateur**

```
sudo tctl users add Administrateur --roles=editor,access
--logins=root,debian
```

Cette commande retournera une sortie similaire à celle-ci :

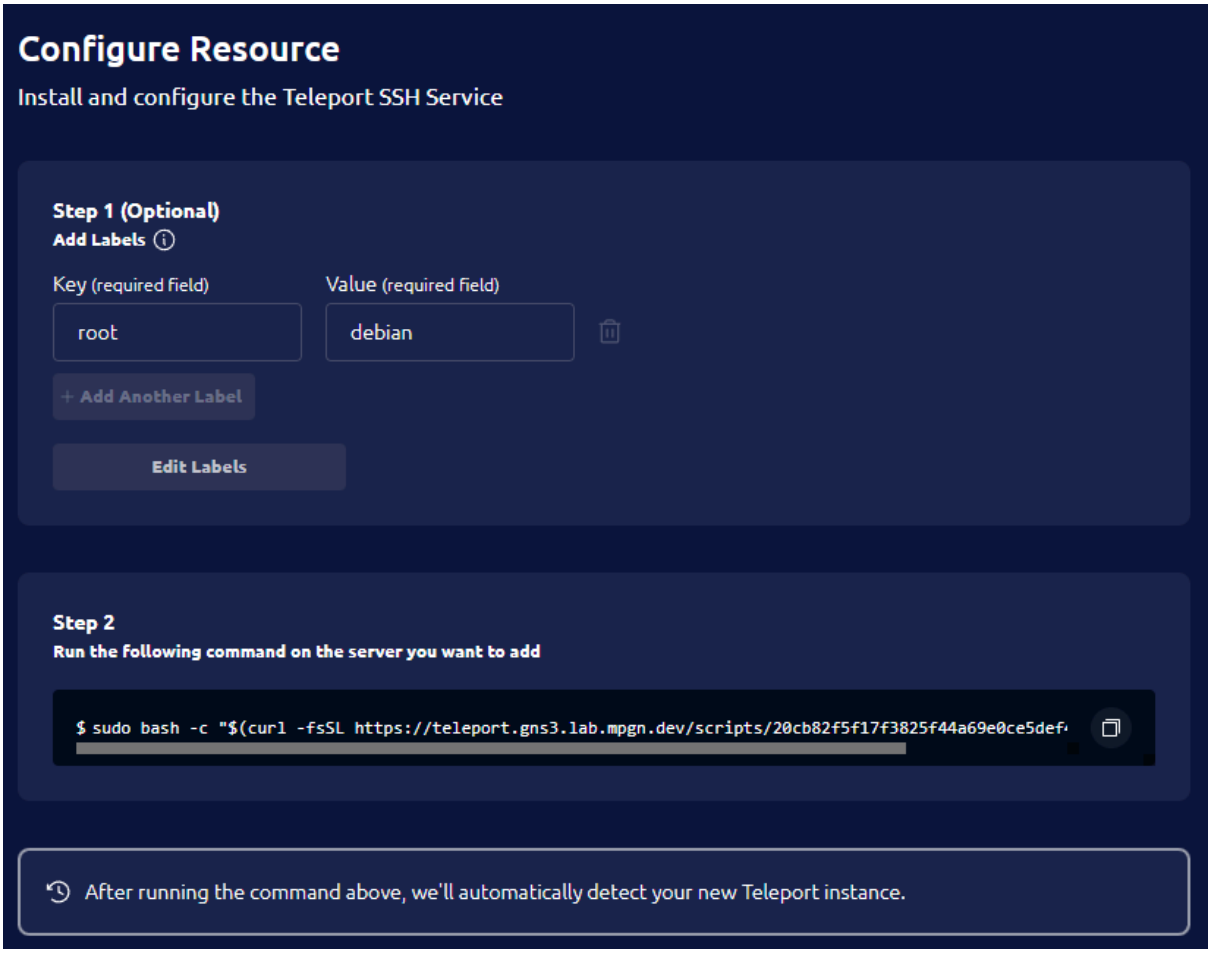
```
User "admin.fb" has been created but requires a password. Share
this URL with the user to complete user setup, link is valid for
1h:
https://teleport.gns3.lab.mpgn.dev:443/web/invite/46d49a7b4456c542
1a2628bdcabe41c4
NOTE: Make sure teleport.gns3.lab.mpgn.dev:443 points at a
Teleport proxy which users can access.
```

2. Installation des Agents Teleport

Les agents Teleport sont installés sur les serveurs (SOC, Services, Front) pour permettre leur gestion centralisée via le bastion.

Étapes d'installation :

1. **Ajouter une ressource :**



3. Vérification des connexions

- Connectez-vous au bastion via HTTPS : `https://teleport.gns3.lab.mpgn.dev/web/cluster/teleport/resources?pinnedOnly=false`
- Vérifiez que les agents sont visibles dans l'interface.

4. Script d'ajout d'utilisateurs et des OU

creation UO et usei Powershell

```powershell
# Importer le module Active Directory
Import-Module ActiveDirectory

# DÃ©finir le mot de passe commun
$SecurePassword = ConvertTo-SecureString "Azertyuiop97420" -AsPlainText -Force

# Liste des OUs Ã  crÃ©er
$OUs = @(
    "Marins",
    "Administratifs",
    "Maintenance",
    "Direction",
    "Informatique"
)

# CrÃ©er les OUs
foreach ($OU in $OUs) {
    $OUPath = "OU=$OU,DC=bluewave,DC=lan"
    if (-not (Get-ADOrganizationalUnit -Filter {Name -eq $OU} -ErrorAction SilentlyContinue))
{
        New-ADOrganizationalUnit -Name $OU -Path "DC=bluewave,DC=lan"
        Write-Host "OU '$OU' crÃ©Ã©e avec succÃ¨s."
    } else {
        Write-Host "OU '$OU' existe dÃ©jÃ ."
    }
}

# Liste des utilisateurs Ã  crÃ©er
$Users = @(
    # Marins
    @{Nom="Dupont"; Prenom="Jean"; OU="Marins"},
    @{Nom="Leclerc"; Prenom="Marie"; OU="Marins"},
    @{Nom="Bernard"; Prenom="Pierre"; OU="Marins"},

    # Administratifs
    @{Nom="Martin"; Prenom="Claire"; OU="Administratifs"},
    @{Nom="Robert"; Prenom="Lucie"; OU="Administratifs"},
    @{Nom="Petit"; Prenom="Nicolas"; OU="Administratifs"},

    # Maintenance
    @{Nom="Durand"; Prenom="Paul"; OU="Maintenance"},
    @{Nom="Morel"; Prenom="Julien"; OU="Maintenance"},
    @{Nom="Girard"; Prenom="Laura"; OU="Maintenance"},

    # Direction
    @{Nom="Lemoine"; Prenom="Sophie"; OU="Direction"},
    @{Nom="Chevalier"; Prenom="Antoine"; OU="Direction"},
    @{Nom="Perrin"; Prenom="Isabelle"; OU="Direction"},

    # Informatique
    @{Nom="Blanc"; Prenom="Thomas"; OU="Informatique"},
    @{Nom="Noir"; Prenom="AmÃ©lie"; OU="Informatique"},
    @{Nom="Gris"; Prenom="Victor"; OU="Informatique"}
)

# CrÃ©er les utilisateurs
foreach ($User in $Users) {
    $UserName = "$($User.Prenom).$($User.Nom)"
    $OUPath = "OU=$($User.OU),DC=bluewave,DC=lan"
    $DisplayName = "$($User.Prenom) $($User.Nom)"

    if (-not (Get-ADUser -Filter {SamAccountName -eq $UserName} -ErrorAction
SilentlyContinue)) {
        New-ADUser -SamAccountName $UserName `
                   -UserPrincipalName "$UserName@bluewave.lan" `
                   -Name $DisplayName `
                   -GivenName $User.Prenom `
                   -Surname $User.Nom `
                   -Path $OUPath `
                   -AccountPassword $SecurePassword `
                   -Enabled $true
        Write-Host "Utilisateur '$DisplayName' crÃ©Ã© avec succÃ¨s dans l'OU '$($User.OU)'."
    } else {
        Write-Host "Utilisateur '$DisplayName' existe dÃ©jÃ ."
    }
}
```