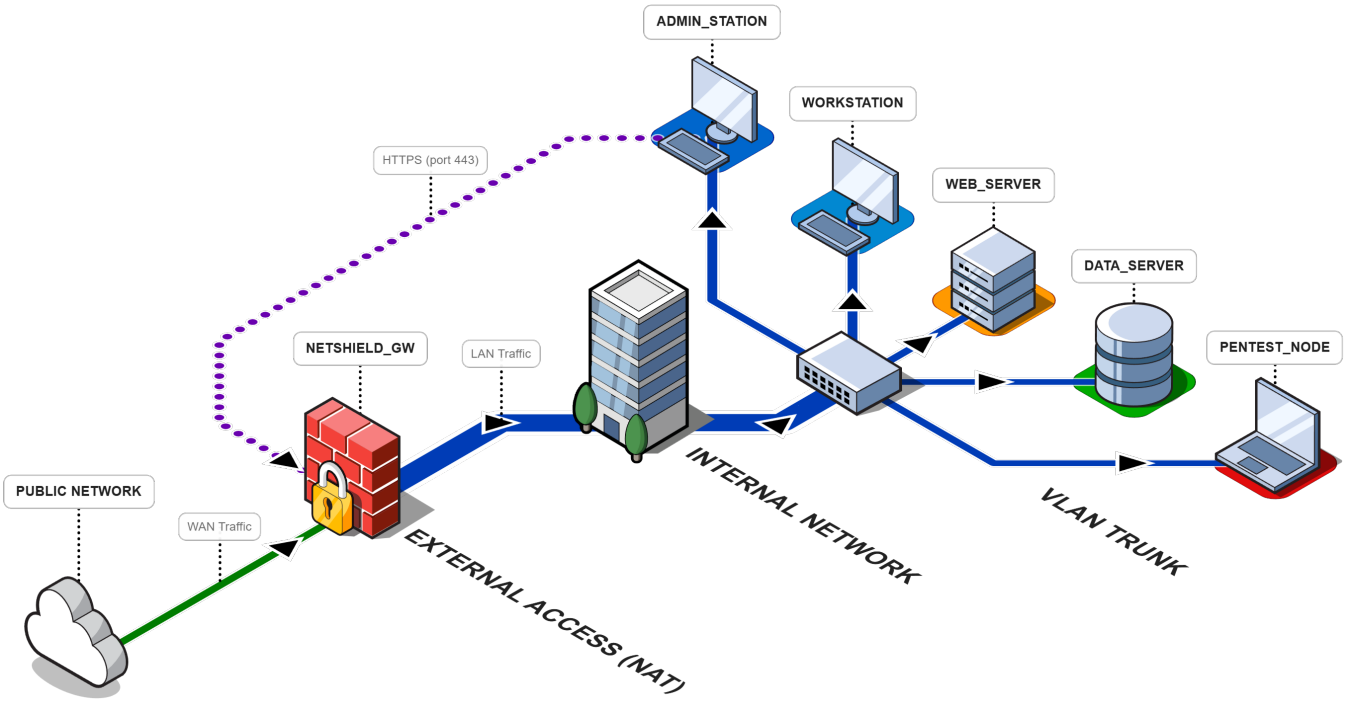
Conception, Sécurisation et Audit d'une Infrastructure Réseau d'Entreprise Segmentée sous pfSense



Projet personnel : Réalisation d'un Home Lab Réseaux et Sécurité incluant segmentation isolée, services serveurs et tests d'intrusion

Wissem KAOUSS

25 février 2026

Table des matières

I Introduction

1 Contexte et Objectifs du projet

Dans le cadre d'une démarche d'auto-formation et de spécialisation en réseaux et cybersécurité, j'ai entrepris la conception et la réalisation d'un *home-lab*. Il s'agit d'un environnement informatique personnel et isolé, permettant de simuler, tester et expérimenter des technologies réseau et de sécurité dans des conditions proches de la réalité, sans risque pour des infrastructures de production.

L'objectif principal de ce projet est de modéliser une infrastructure d'entreprise moderne en intégrant les principes fondamentaux de la défense en profondeur. Ce projet s'articule autour de la segmentation réseau par VLANs, de la mise en place d'une politique de filtrage via un pare-feu pfSense, et de l'hébergement de services critiques tels qu'un serveur web et un stockage de données.

Au-delà de l'aspect constructif, ce laboratoire a pour vocation de servir de terrain d'audit. En simulant des attaques via une distribution Kali Linux, l'enjeu est d'identifier les vecteurs d'intrusion potentiels afin de déployer des solutions de remédiation adaptées, telles que des systèmes de prévention d'intrusion ou le durcissement des services exposés. Cette approche itérative permet ainsi de valider l'efficacité des mesures de protection mises en œuvre.

2 Présentation du Home Lab

L'infrastructure repose sur un environnement entièrement virtualisé à l'aide de l'hyperviseur de type 2 **Oracle VM VirtualBox**. Ce choix permet de simuler l'interconnexion de plusieurs réseaux hétérogènes sur une machine hôte unique, tout en garantissant une isolation stricte entre les machines virtuelles (*VM*). Le cœur du dispositif est le pare-feu pfSense, qui assure le rôle de passerelle centrale (*Gateway*) et de gestionnaire de flux.

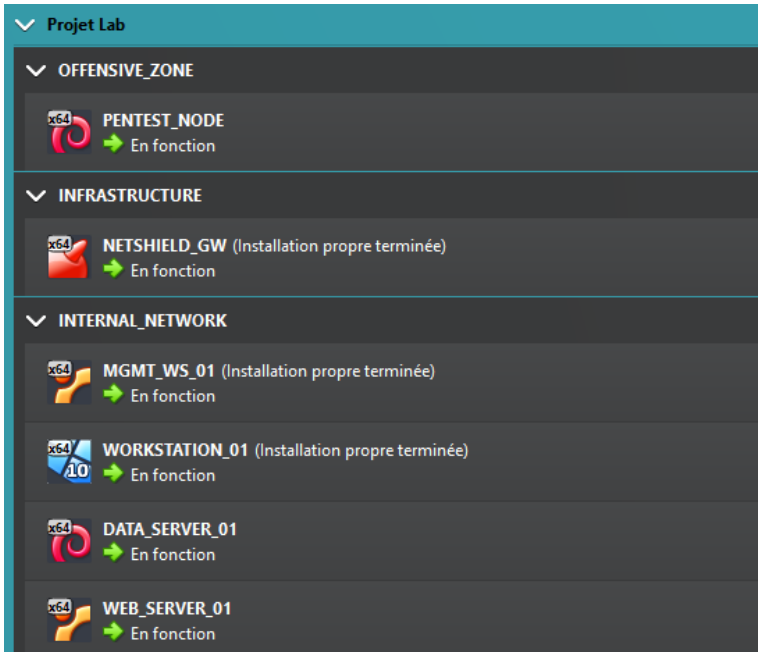


Figure 1 – Liste des VM

La topologie retenue (voir Figure 2) illustre une architecture d'entreprise classique et hiérarchisée. Le trafic est centralisé via un commutateur de cœur de réseau virtuel, assurant la liaison logique entre les différents segments et le pare-feu. L'architecture se décline en plusieurs zones distinctes :

— Un accès extérieur (**WAN**) protégé permettant la sortie vers internet ;
— Une zone de gestion (**MGMT**) pour l'administration sécurisée de l'infrastructure ;
— Un segment dédié aux utilisateurs (**USERS**) pour les postes de travail ;
— Une zone démilitarisée (**DMZ**) isolant les services exposés, tel qu'un serveur web ;
— Un segment de stockage (**STORAGE**) dédié à la persistance des données ;
— Une zone d'audit (**AUDIT**) isolée, destinée à tester la robustesse de cette structure via des outils de test d'intrusion.

Cette organisation permet d'appliquer les concepts de segmentation et d'isolation (*sandboxing*) dès la conception du réseau. Une attention particulière est portée à la **Zone Démilitarisée (DMZ)** : il s'agit d'un sous-réseau tampon isolé du réseau local interne, mais accessible depuis l'extérieur. Son rôle est de contenir les services exposés (ici, le serveur Web) afin qu'une éventuelle compromission de ces services n'affecte pas l'intégrité des zones critiques, comme les segments de gestion ou de stockage. Cette approche garantit ainsi une défense en profondeur, limitant drastiquement la portée d'une intrusion.

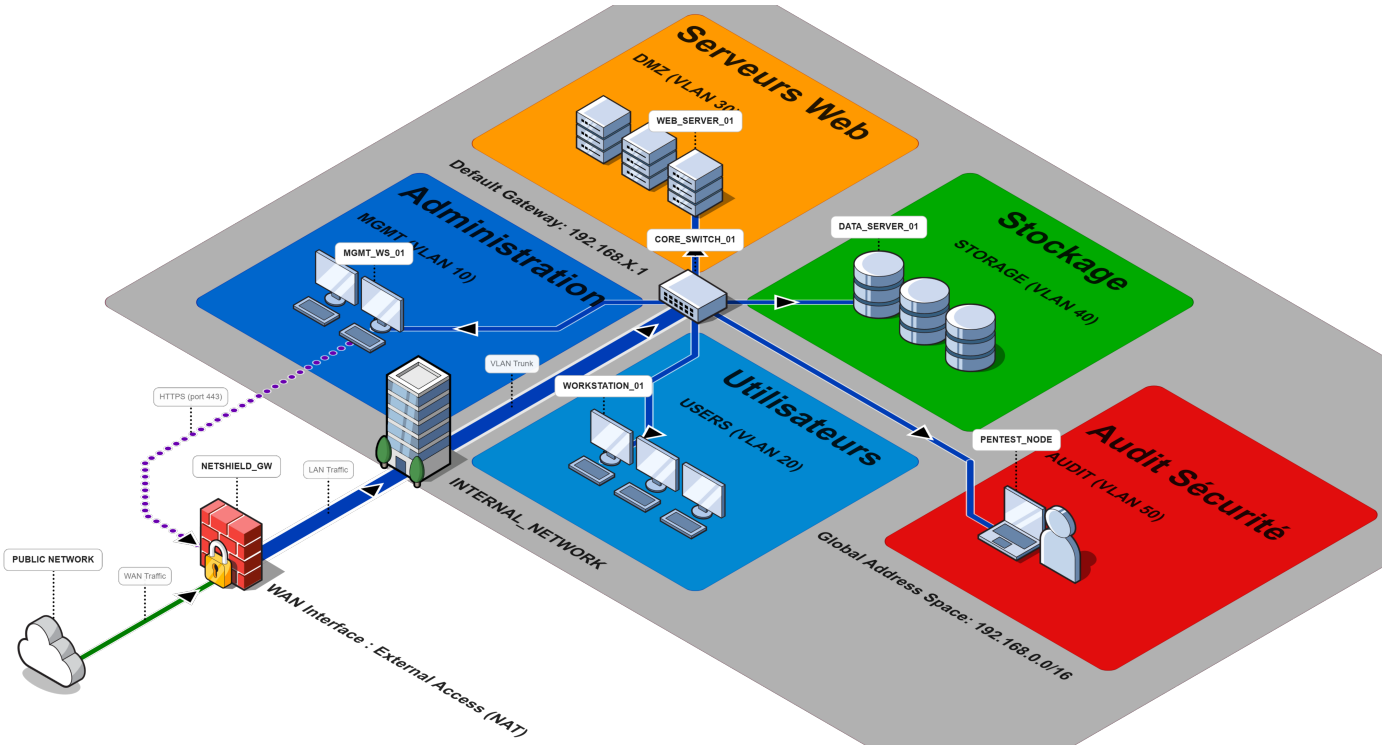


FIGURE 2 – Topologie logique de l'infrastructure segmentée

II Architecture Réseau et Plan d'Adressage

1 Topologie de l'infrastructure

L'architecture de ce projet repose sur une topologie en étoile, plaçant le pare-feu pfSense au centre du dispositif. Ce choix garantit que chaque flux de données entre les différents segments réseau soit systématiquement soumis à l'inspection et aux politiques de filtrage définies sur la passerelle.

La connectivité réseau repose sur une architecture en **Full Trunk** s'appuyant sur la norme **IEEE 802.1Q**. Contrairement à une approche "multi-câble" où chaque segment nécessiterait une interface réseau physique (ou virtuelle) dédiée sur le pare-feu, le mode Trunk permet de mutualiser l'ensemble des flux sur un lien unique à haut débit.

Ce lien relie virtuellement l'interface LAN du pare-feu au `CORE_SWITCH`. Ce dernier agit comme un commutateur virtuel supportant le trunking *(agrégation de flux)*, permettant de transporter les trames étiquetées *(VLAN tagging)* vers le pare-feu. Cette méthode offre une flexibilité maximale : l'ajout d'un nouveau réseau ne nécessite aucune modification de l'infrastructure matérielle, mais une simple configuration logicielle au sein du pare-feu et de l'hyperviseur.

Cette organisation structure le réseau de manière professionnelle, permettant de simuler un environnement de production où la centralisation du contrôle est primordiale pour la sécurité globale de l'infrastructure.

2 Segmentation par VLANs

La segmentation constitue le socle de sécurité de cette architecture. Elle permet de limiter les domaines de diffusion et de contrôler strictement les flux via le pare-feu. Pour ce projet, j'ai adopté un découpage basé sur le standard **192.168.X.0/24**, où chaque troisième octet identifie de manière unique le segment concerné.

Afin de maintenir une structure d'adressage homogène, la passerelle par défaut (*default gateway*) de chaque sous-réseau est systématiquement positionnée sur la première adresse disponible, soit le suffixe **.1** (par exemple, **192.168.10.1** pour le VLAN `MGMT`). Cette convention facilite l'administration et la configuration du routage inter-VLAN.

Une configuration spécifique a été appliquée à l'interface LAN physique : par défaut, tout équipement non assigné est positionné sur le segment `USERS (VLAN 20)`. Cette approche permet d'appliquer immédiatement une politique de filtrage standard avant toute élévation de privilèges ou changement de segment.

La capture d'écran suivante (Figure 3) présente l'implémentation de ces segments au sein de l'interface pfSense, illustrant la correspondance entre les tags VLAN et les interfaces logiques.

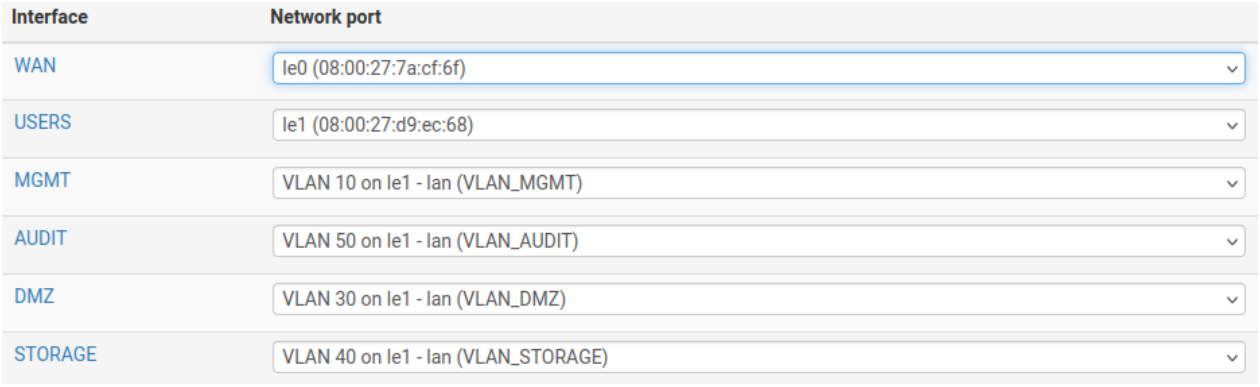


FIGURE 3 – Configuration des interfaces logiques et des tags VLAN sur pfSense

3 Détail des hôtes et plan d'adressage

Le tableau ci-dessous synthétise le plan d'adressage IP statique utilisé pour les différentes machines du laboratoire. Cette précision est indispensable pour configurer les règles de filtrage que nous détaillerons dans la partie suivante.

Hostname	**VLAN**	**Adresse IP**	**Rôle / Fonction**
NETSHIELD_GW	WAN	10.0.2.15 (NAT)	Interface externe (Accès Internet)
	LAN (Trunk)	192.168.X.1	Passerelle par défaut des VLANs
MGMT_WS_01	10	192.168.10.10	Administration (Linux Mint)
WORKSTATION_01	20	192.168.20.10	Poste utilisateur (Windows 10)
WEB_SERVER_01	30	192.168.30.10	Serveur Web (Ubuntu Server)
DATA_SERVER_01	40	192.168.40.10	Stockage (OpenMediaVault)
PENTEST_NODE	50	192.168.50.10	Audit (Kali Linux)

TABLE 1 – Synthèse du plan d'adressage et des systèmes d'exploitation

III Déploiement des Services et Gestion des Hôtes

1 Administration et Postes de Travail

Le pilotage de l'infrastructure est centralisé sur le poste `MGMT_WS_01` (VLAN 10). Cette machine sous Linux Mint fait office de station d'administration sécurisée. C'est depuis cet hôte, et exclusivement à travers l'adresse IP `192.168.10.1`, que l'interface de gestion Web du pare-feu pfSense est accessible. Ce cloisonnement garantit que les fonctions critiques de configuration du réseau sont isolées des autres utilisateurs.

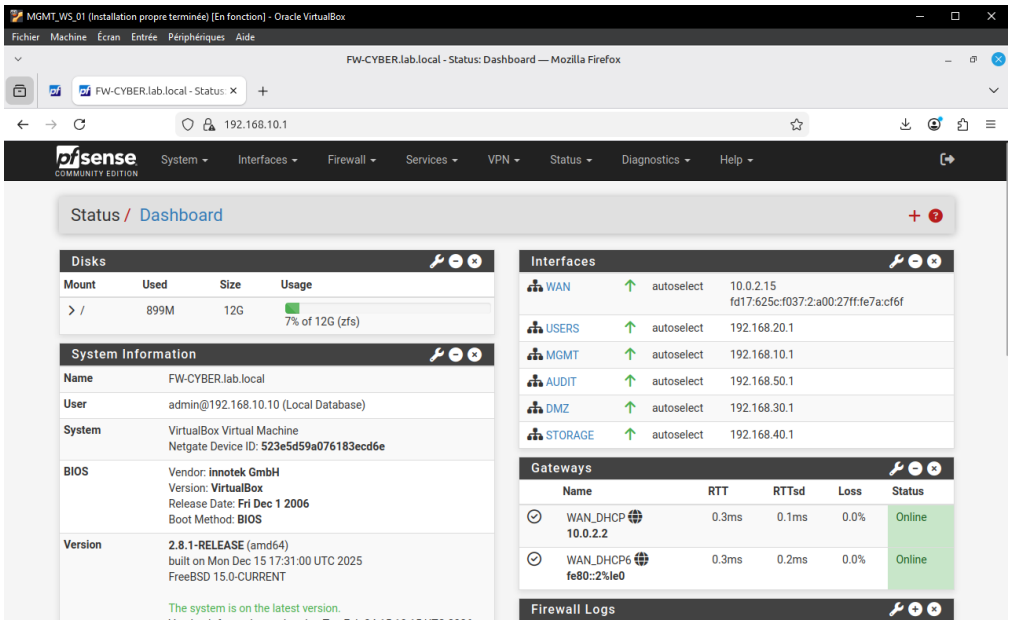


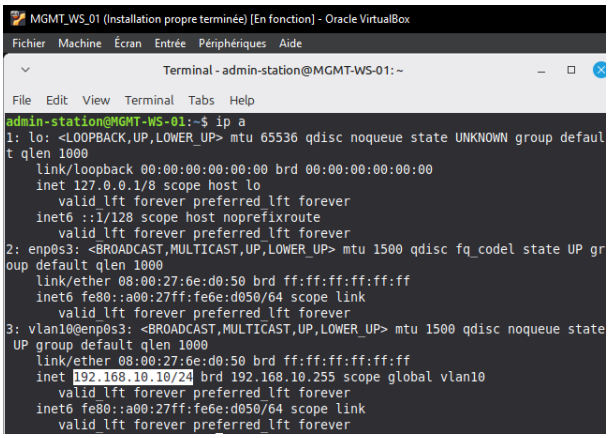
FIGURE 4 – Aperçu du dashboard de pfSense

À l'inverse, la machine `WORKSTATION_01` (VLAN 20) simule le poste de travail d'un employé au sein de l'entreprise. Sous Windows 10, cet hôte est destiné aux tâches bureautiques quotidiennes et bénéficie d'un accès à Internet pour les besoins métiers, tout en étant strictement limité dans ses interactions avec les segments sensibles du réseau (DMZ, Stockage, Gestion).

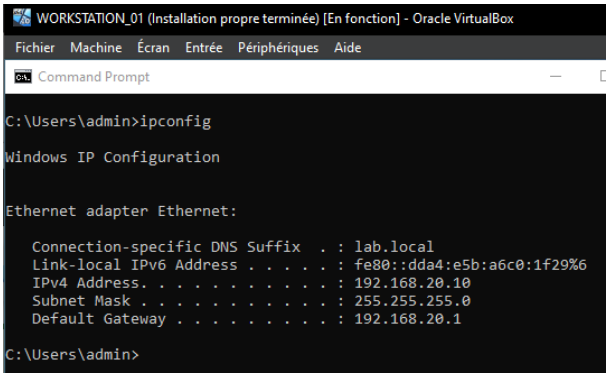
2 Automatisation de l'adressage (Service DHCP)

Le processus d'intégration d'une nouvelle machine suit une logique rigoureuse de segmentation dynamique :

- **Raccordement au switch :** La machine virtuelle est assignée au réseau interne géré par l'hyperviseur.
- **Assignation par défaut (VLAN Natif) :** Par défaut, toute nouvelle interface non configurée est placée dans le segment `USERS` (VLAN 20). Cela garantit qu'un hôte ne peut pas accéder aux segments sensibles (Administration ou Stockage) sans une intervention explicite.
- **Configuration de l'hôte :** Pour déplacer une machine dans un autre segment, le port correspondant sur le `CORE_SWITCH` est reconfiguré avec le tag VLAN approprié.
- **Attribution DHCP :** Une fois le segment identifié, le serveur DHCP de pfSense intercepte la requête de la machine et lui attribue une adresse IP correspondant à son VLAN (ex : `192.168.20.X` pour un utilisateur ou `192.168.10.X` pour l'administration), ainsi que l'adresse de sa passerelle par défaut en `.1`.



(a) Attribution de l'IP `192.168.10.10` (VLAN 10) à l'hôte `MGMT_WS_01`



(b) Attribution de l'IP `192.168.20.10` (VLAN 20) à l'hôte `WORKSTATION_01`

FIGURE 5 – Preuve de fonctionnement du service DHCP inter-VLAN

3 Centralisation des données et service Web

L'utilité de cette infrastructure repose sur la mise à disposition d'un stockage centralisé et d'un service de diffusion Web. Pour ce faire, une solution **OpenMediaVault (OMV)** a été déployée dans le segment STORAGE. Elle héberge un dossier partagé accessible par l'ensemble des hôtes du réseau.

D'un point de vue technique, le partage de fichiers a été implémenté via le protocole **SFTP** plutôt que via les protocoles classiques NFS ou SMB. Ce choix est motivé par la simplicité de sécurisation à travers le pare-feu (utilisation d'un port unique) et le chiffrement natif des données. Pour lier le serveur Web au stockage, j'ai utilisé l'outil **SSHFS** (*SSH Filesystem*), permettant de monter le répertoire distant d'OMV directement dans l'arborescence du serveur Nginx de manière transparente et sécurisée.

Cependant, l'accès à ces données est régi par une politique de droits d'accès stricte (ACL - *Access Control Lists*). Comme illustré dans la Figure 6, j'ai créé un groupe `users` et un compte utilisateur dédié (`user_lab`). LLes permissions ont été configurées de manière restrictive : seul ce groupe possède les droits de lecture/écriture sur le répertoire partagé, interdisant ainsi tout accès non autorisé, même en provenance d'un hôte situé dans le même segment réseau.

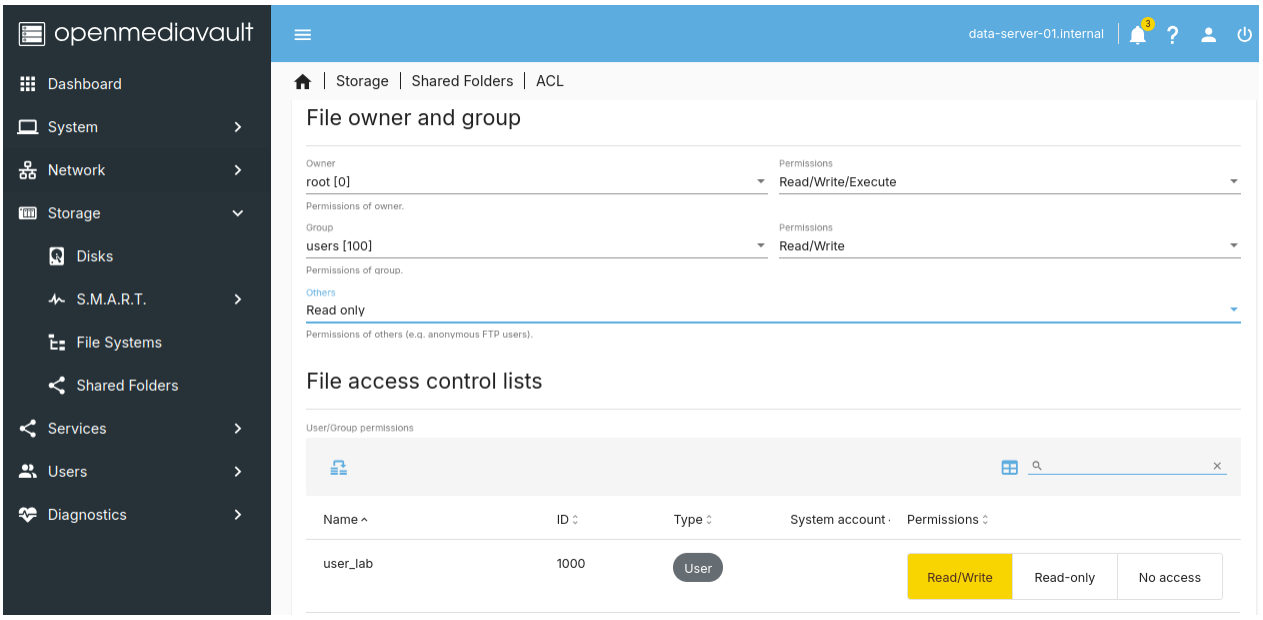


FIGURE 6 – Configuration des privilèges et ACL sur l'interface OpenMediaVault

La preuve de la synchronisation et de l'accessibilité de ce stockage est illustrée par la Figure 7, où l'on observe la persistance des mêmes fichiers entre le poste d'administration (Linux) et le poste utilisateur (Windows).

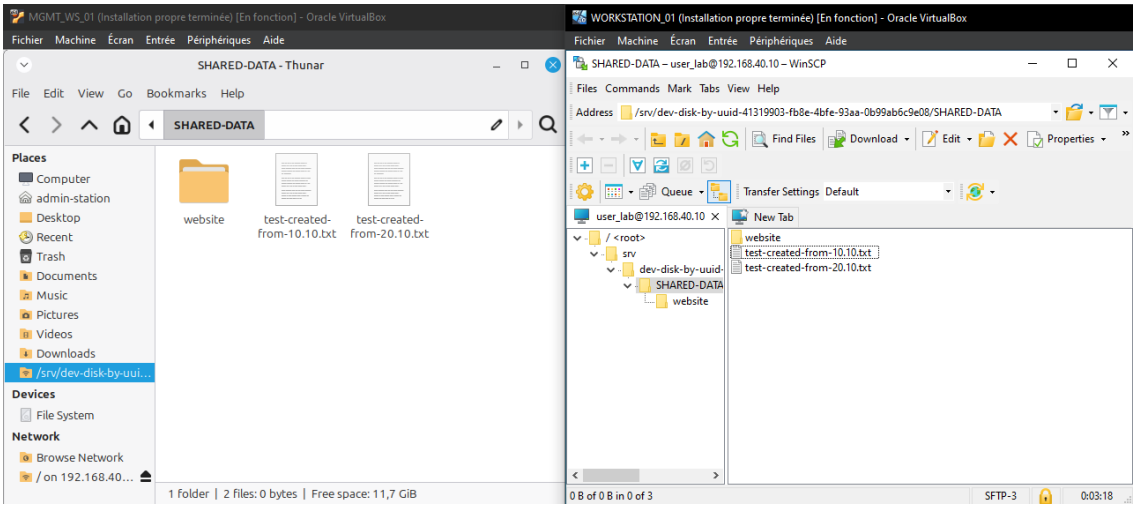


FIGURE 7 – Accès partagé au serveur OMV depuis les segments `MGMT` et `USERS`

Le serveur Web **Nginx**, situé en `DMZ`, exploite également cette centralisation. Au sein du dossier partagé, un sous-répertoire spécifique nommé `website` contient les fichiers du site. Afin de lier le service Web à ces données, j'ai modifié le fichier de configuration `/etc/nginx/sites-available/default` pour redéfinir la racine du serveur (*root directory*) vers le chemin local `/var/www/html/website` (où est monté le partage SFTP).

Comme le montre la Figure 8, le poste Windows peut ainsi consulter la page d'accueil du site, prouvant que le flux est correctement acheminé du segment `USERS` vers la `DMZ`, laquelle récupère ses données dans le segment STORAGE.

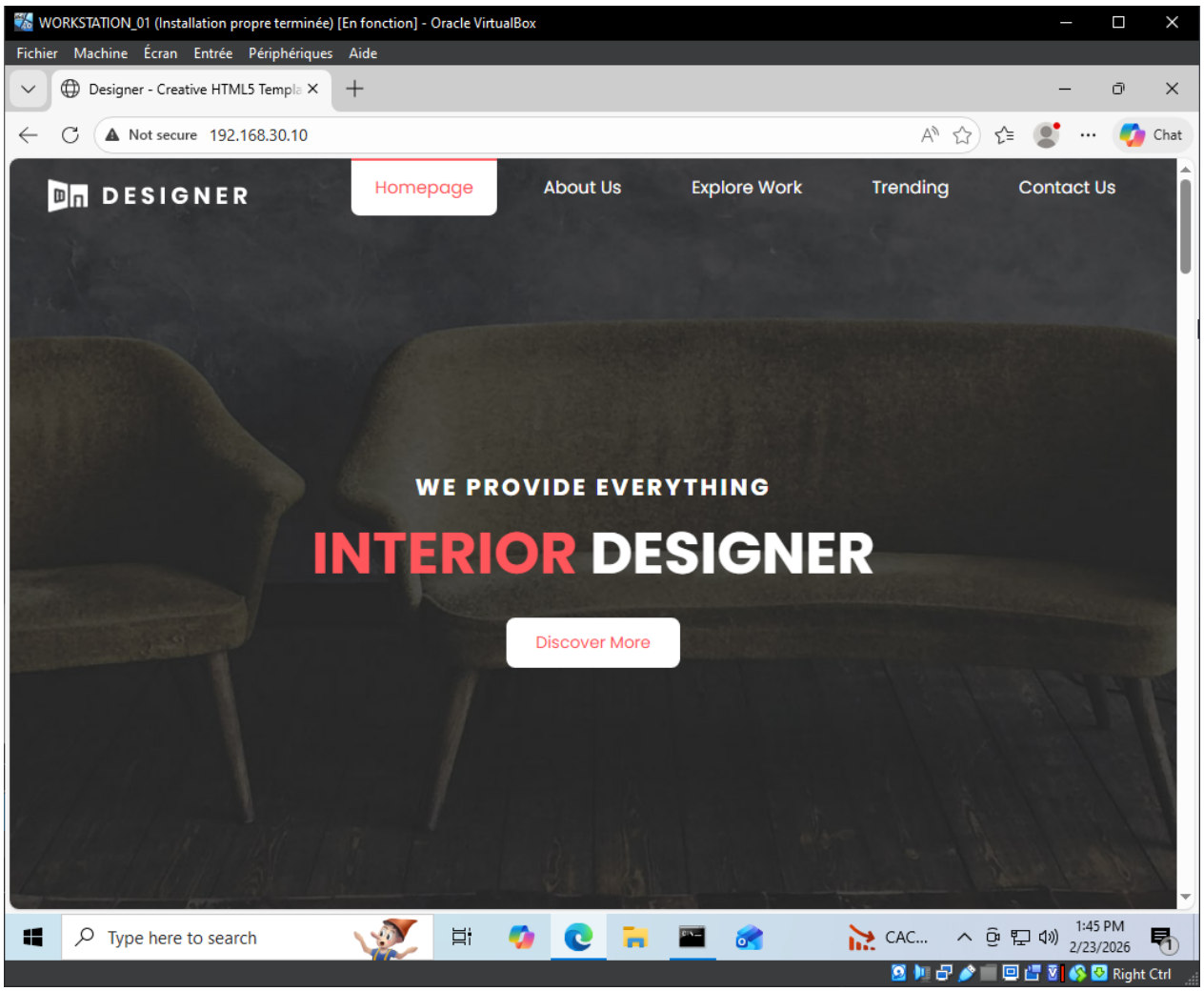


FIGURE 8 – Accès à la page d'accueil du serveur Web depuis le poste Windows

IV Politique de Filtrage et Sécurisation (pfSense)

La sécurité du laboratoire repose sur une politique de filtrage *Stateful* (à état) appliquée sur chaque interface de VLAN. L'objectif est de garantir que chaque flux réseau répond à un besoin métier, tout en interdisant par défaut tout trafic non autorisé (*Default Deny*), *"tout ce qui n'est pas autorisé est interdit"*.

1 Segment USERS : Un accès filtré et orienté vers l'extérieur

Le segment des utilisateurs présente la surface d'exposition la plus importante en raison de son accès à Internet. Sa configuration vise à offrir les ressources nécessaires à la productivité tout en interdisant strictement toute navigation latérale vers les segments critiques comme l'administration ou le stockage.

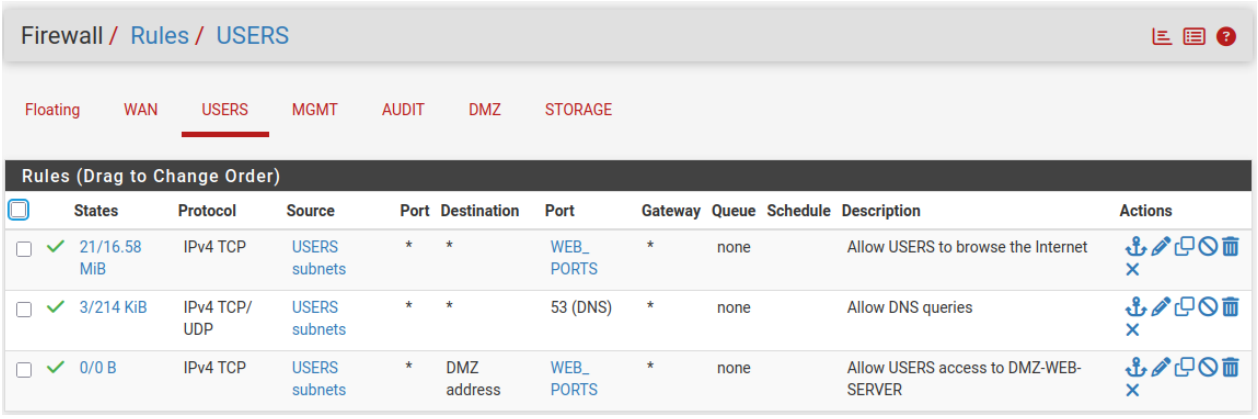


FIGURE 9 – Règles de filtrage du segment `USERS` (VLAN 20)

Comme illustré en Figure 9, trois règles fondamentales régissent ce segment :

- **Résolution de noms (DNS) :** Autorisation du port 53 (UDP/TCP) vers l'extérieur pour permettre la traduction des domaines.
- **Flux métiers vers la DMZ :** L'accès au serveur Web interne est autorisé via un alias limitant le trafic aux ports standards (80/443), isolant ainsi l'utilisateur des autres services de la zone démilitarisée.
- **Navigation Internet :** Un flux vers toute destination (`*`) est autorisé, mais limité aux ports Web standards via un alias, évitant ainsi l'utilisation de protocoles non autorisés.

2 Segment MGMT : Une zone d'administration isolée et restrictive

Le segment d'administration est le cœur de l'infrastructure. Contrairement aux autres zones, il est totalement dépourvu d'accès à Internet, réduisant ainsi drastiquement les risques d'exfiltration de données ou de compromission via des vecteurs externes. Ses accès vers les autres segments sont définis pour répondre aux besoins exclusifs de gestion.

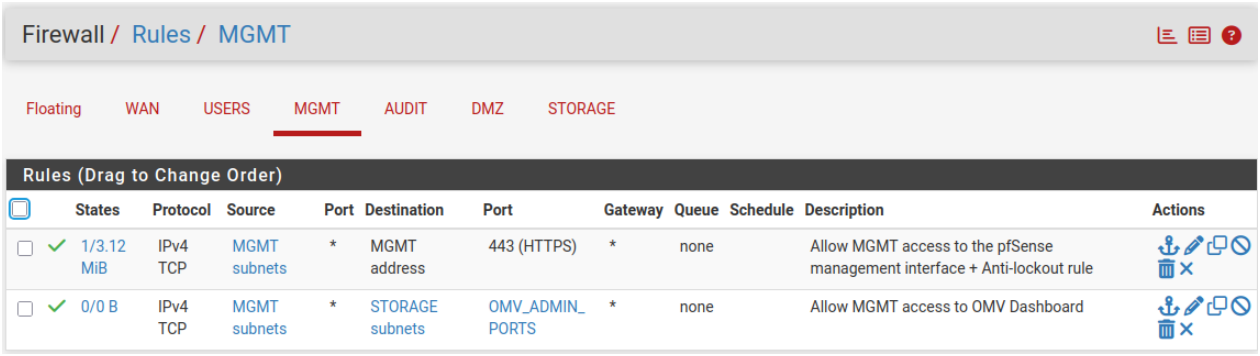


FIGURE 10 – Règles de filtrage du segment `MGMT` (VLAN 10)

Deux règles stratégiques définissent la sécurité de cette zone (Figure 10) :

- **Gestion du Stockage (VLAN 40) :** L'accès au serveur OMV est filtré par l'alias `OMV_ADMIN_PORTS`. Cela limite la communication aux ports 22 (SSH/SFTP), 80 et 443. L'administrateur peut ainsi gérer les fichiers et l'interface Web sans exposer d'autres services vulnérables.
- **Interface pfSense (Anti-Lockout) :** L'accès à l'interface de gestion du pare-feu est restreint au port 443 (HTTPS) vers l'adresse IP de la passerelle. Cette règle manuelle remplace la règle automatique par défaut, garantissant que seul un hôte du VLAN 10 peut configurer le cœur de réseau.

V Audit de Sécurité et Tests d'Intrusion (Pentest)

Cette section documente la phase de validation de l'infrastructure. À l'aide d'une instance **Kali Linux** (`PENTEST-NODE`) positionnée dans le segment `AUDIT` (VLAN 50), j'ai simulé une intrusion pour éprouver le cloisonnement du pare-feu et la robustesse des services.

1 Préparation de l'environnement d'audit

La phase d'audit débute par l'intégration de la machine `PENTEST-NODE` au segment dédié. Pour simuler un intervenant extérieur, j'ai configuré une interface virtuelle tagguée sur le VLAN 50 via la commande :

```
sudo nmcli con add type vlan con-name "VLAN_AUDIT" dev eth0 id 50
```

Cette configuration applique l'encapsulation 802.1Q nécessaire à la carte physique. Après activation du profil et déconnexion de l'interface `eth0` pour éviter tout conflit de routage, la machine a obtenu l'adresse `192.168.50.10` par DHCP. La connectivité a été validée par un `ping` réussi vers la passerelle par défaut (`192.168.50.1`), confirmant que l'auditeur est opérationnel mais strictement contraint par les règles de filtrage du pfSense.

2 Test 1 : Reconnaissance et étanchéité du cloisonnement

L'objectif est ici de vérifier que le pare-feu applique correctement les politiques de flux, en autorisant les audits légitimes tout en bloquant les tentatives d'intrusion sur les segments protégés.

a Scan de la DMZ (Flux autorisé pour l'audit)

Pour permettre l'évaluation de la surface d'attaque du serveur Web, une règle spécifique a été créée sur l'interface `AUDIT`. Concrètement, cette règle lève temporairement l'isolation du VLAN 50 pour simuler une machine d'attaque ayant réussi à s'introduire sur le réseau.

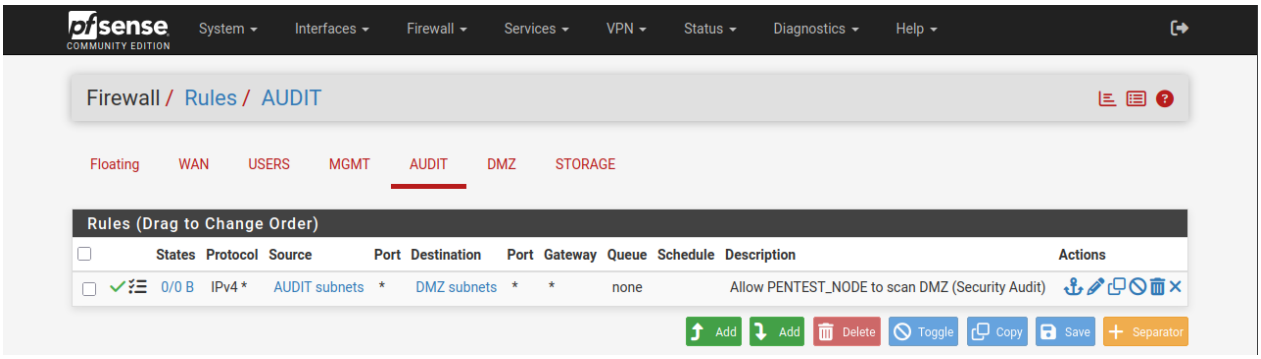
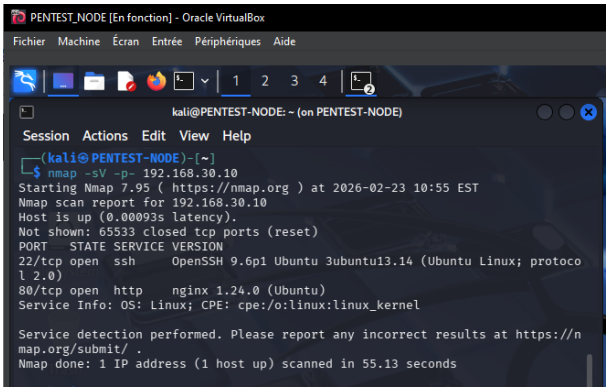
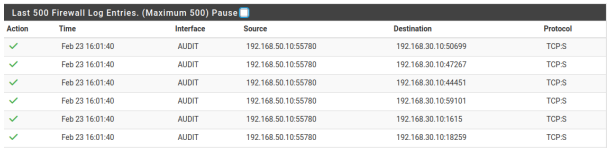


FIGURE 11 – Configuration de la règle d'audit autorisant le trafic vers la `DMZ`

Le scan agressif `nmap -sV -p- 192.168.30.10` a identifié les ports **22 (SSH)** et **80 (HTTP)** comme ouverts. La remontée des versions (Nginx 1.24.0 et OpenSSH 9.6p1) confirme que le trafic traverse le pare-feu sans altération. Cette visibilité totale permet une identification ciblée des vulnérabilités potentielles liées à ces services.



(a) Identification des services par Nmap

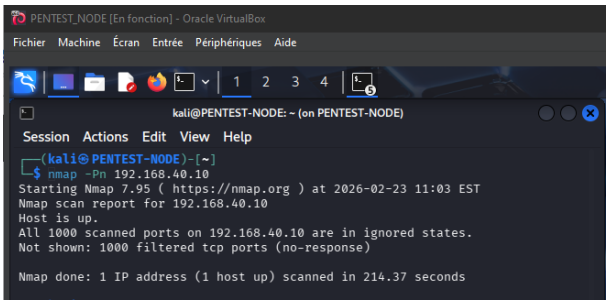


(b) Flux autorisés dans les journaux pfSense

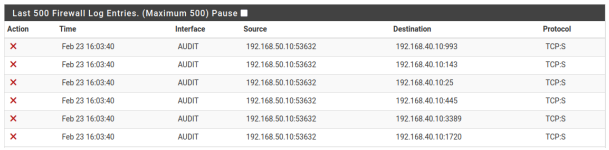
FIGURE 12 – Validation de l'ouverture des flux vers le segment `DMZ`

b Scan du segment STORAGE (Flux interdit par défaut)

Une tentative de reconnaissance a ensuite été menée vers le serveur de stockage (`192.168.40.10`). Contrairement au test précédent, aucune règle n'autorise le VLAN 50 à communiquer avec le VLAN 40.



(a) Résultat du scan : ports filtrés



(b) Blocage des tentatives de scan (TCP Stealth)

FIGURE 13 – Preuve du cloisonnement strict entre le VLAN `AUDIT` et le VLAN `STORAGE`

On observe que Nmap indique `1000 filtered tcp ports` et le test ICMP (Ping) se solde par une perte de paquets de 100%. Le comportement du pfSense, fondé sur le mode **DROP** (silence radio), est privilégié ici pour ne donner aucune indication sur l'existence d'une cible active.

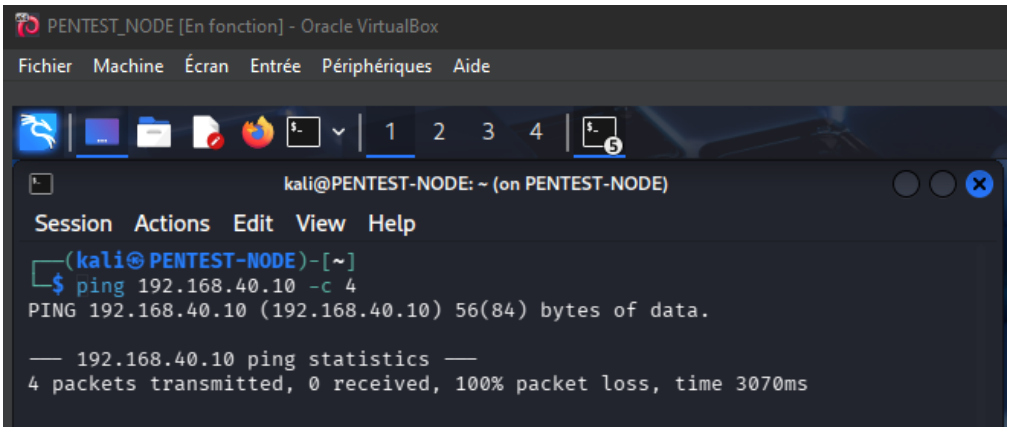


FIGURE 14 – Échec de la connectivité ICMP : isolation réseau confirmée

3 Test 2 : Attaque par force brute et durcissement applicatif

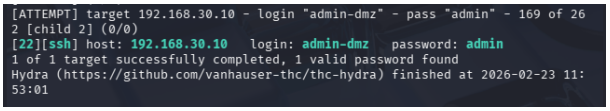
Le passage de la reconnaissance à l'exploitation suit une méthodologie structurée. Après avoir identifié le port 22 comme vecteur d'entrée, l'attaquant tente d'obtenir un accès initial pour envisager, par la suite, un rebond réseau ou une exfiltration de données.

a Exécution de l'attaque avec Hydra

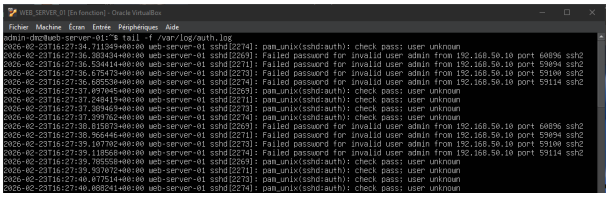
J'ai lancé une attaque par dictionnaire contre l'utilisateur `admin-dmz` afin de tester une *wordlist* de manière automatisée :

```
hydra -l admin-dmz -P /usr/share/wordlists/fasttrack.txt ssh://192.168.30.10 -t 4 -V
```

En quelques secondes, l'outil a découvert le mot de passe par défaut, soulignant une vulnérabilité critique liée à la faiblesse des identifiants.



(a) Succès de l'attaque Hydra



(b) Logs du serveur enregistrant les échecs

FIGURE 15 – Phase d'exploitation du service SSH

b Exploitation : Rebond et impact métier

Une fois l'accès obtenu, le cloisonnement réseau peut être contourné par un "rebond" applicatif via le montage **SSHFS**. En tant qu'attaquant, j'ai pu naviguer dans `/mnt/storage` et accéder aux données confidentielles de l'unité de stockage. Cet accès a permis de réaliser une défiguration (*Defacement*) en modifiant les fichiers sources du site web hébergés à distance, impactant directement le service rendu aux utilisateurs.

Ce scénario illustre le principe de l'escalade de privilèges : le pare-feu autorise le flux SSH légitime, mais ne peut distinguer une session d'administration d'une intrusion. La sécurité du segment `STORAGE` dépend donc ici directement de la robustesse du serveur Web.

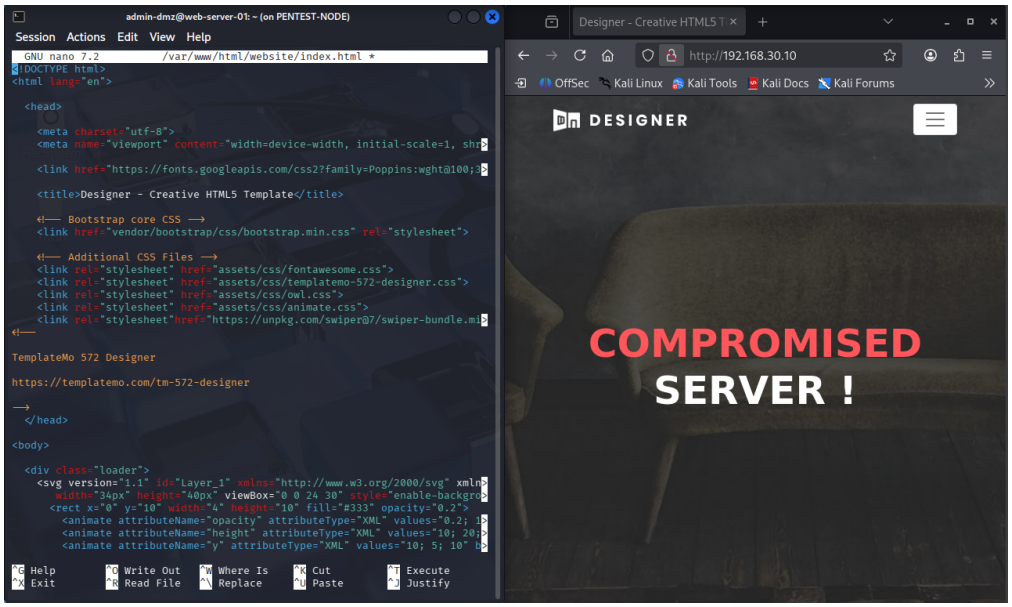


FIGURE 16 – Visualisation du site web altéré après le rebond

c Remédiation : Défense en profondeur

Pour contrer cette menace, deux mesures de durcissement (*hardening*) ont été déployées :

1. **Politique de mots de passe robustes :** Utilisation d'une chaîne complexe de plus de 20 caractères, rendant l'attaque par dictionnaire techniquement impossible.
2. **Bannissement dynamique avec Fail2Ban :** Le service surveille les journaux d'authentification et bannit automatiquement l'IP de l'attaquant après 3 échecs.

```
┌──(kali㉿PENTEST-NODE)-[~]
└─$ hydra -l admin-dmz -P /usr/share/wordlists/fasttrack.txt ssh://192.168.30
.10 -t 4
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 2026-02-23 14:
14:34
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
 waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 262 login tries (l:1/p:262)
, ~66 tries per task
[DATA] attacking ssh://192.168.30.10:22/
[STATUS] 20.00 tries/min, 20 tries in 00:01h, 242 to do in 00:13h, 4 active
[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 2026-02-23 14:
16:52
```

(a) Échec d'Hydra (Mot de passe robuste)

```
WEB_SERVER_01 [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
admin-dmz@web-server-01:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     12
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.50.10
```

(b) IP bannie affichée par Fail2Ban

FIGURE 17 – Mise en œuvre des mesures de défense active

4 Synthèse de l'audit et enseignements

Cet audit démontre que la segmentation réseau via pfSense constitue une première ligne de défense efficace, comme le prouve l'étanchéité du segment `STORAGE`. Cependant, l'expérience souligne qu'un filtrage périmétrique ne peut compenser une faiblesse applicative. La réussite du rebond SSH rappelle l'importance d'une stratégie de **défense en profondeur**. La sécurité globale repose sur la complémentarité entre le cloisonnement (VLANs), le durcissement système et la surveillance active (Fail2Ban), garantissant qu'en cas de défaillance d'un maillon, les ressources critiques restent protégées.

VI Conclusion

Ce projet a permis la conception et la sécurisation d'une infrastructure virtualisée répondant aux exigences d'une architecture d'entreprise. Au-delà de l'aspect déploiement, ce laboratoire a servi de cadre d'analyse pour éprouver les mécanismes de défense face à des vecteurs d'attaque.

1 Bilan technique et enseignements de l'audit

L'audit mené avec Kali Linux a confirmé la robustesse de la segmentation réseau opérée par pfSense. L'étanchéité inter-VLAN, régie par une politique *Default Deny*, a neutralisé toute tentative de reconnaissance directe vers le segment `STORAGE`. Cependant, l'exploitation réussie du service SSH a mis en évidence le risque lié au **mouvement latéral** (*Lateral Movement*). En compromettant le serveur Web via une attaque par dictionnaire, j'ai pu utiliser la relation de confiance existante (montage SSHFS) pour accéder à l'unité de stockage, contournant ainsi le filtrage périmétrique.

Ce scénario souligne qu'une intrusion ne nécessite pas systématiquement une **escalade de privilèges** (*Privilege Escalation*) complexe si les identifiants initiaux sont faibles. La sécurité repose donc sur la complémentarité entre le cloisonnement réseau, le durcissement du système hôte et la surveillance active via **Fail2Ban**. Cette approche de **défense en profondeur** garantit qu'en cas de compromission d'un maillon, des contre-mesures applicatives prennent le relais pour limiter l'impact métier et protéger les ressources critiques.

2 Perspectives d'évolution

Pour faire évoluer ce laboratoire vers un environnement de production mature, plusieurs axes d'optimisation sont envisageables :

- **Gestion centralisée des identités :** L'intégration d'un serveur **Active Directory** permettrait d'unifier la gestion des droits et d'appliquer des politiques de mots de passe globales, éliminant les vulnérabilités liées aux comptes locaux.
- **Supervision et Observabilité :** Le déploiement d'une solution comme **Zabbix** offrirait une surveillance en temps réel de la charge système et de la disponibilité des services, facilitant la détection proactive d'incidents.
- **Optimisation du stockage et Disponibilité :** La transition vers des protocoles comme **NFS ou iSCSI**, couplée à la mise en place d'un cluster pfSense en haute disponibilité (*Failover*), assurerait une performance accrue et une résilience face aux pannes matérielles.

En résumé, ce projet m'a permis de maîtriser l'ensemble de la chaîne de déploiement d'une infrastructure : de la conception du cœur de réseau (routage, segmentation, filtrage) à la mise en production de services critiques et leur sécurisation applicative. Cette expérience concrète offre la vision transverse indispensable pour concevoir, administrer et protéger un parc informatique moderne, en conciliant les besoins opérationnels de l'entreprise et les impératifs de cybersécurité.