المدرسة الوطنية للعلوم التطبيقية - مراكش
ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES - MARRAKECH
MARRAKECH
جامعة القاضي عياض
UNIVERSITÉ CADI AYYAD
GCDSTE
ENSA MARRAKECH

NAC – CONTRÔLE D'ACCÈS RÉSEAU AVEC PacketFence

Réalisé par:

- Kaoutar El kissany
- Soukaina Bachir
- Bagy Oussama
- Ikram Laabouki
- Hiba Lazzouzi

Encadré par:
Pr.ALI AZOUGAGH

PLAN

01 Contexte & Problématique

02 Objectifs du Projet

03 Présentation du NAC

04 Technologies utilisées

05 Topologie

06 Authentification et test

07 Conformité et test

08 Conclusion

CONTEXTE

Dans les réseaux modernes, de nombreux appareils personnels ou professionnels se connectent chaque jour, ce qui augmente les risques de sécurité. Certains équipements peuvent être non autorisés, mal configurés ou même vulnérables, ce qui peut compromettre l'ensemble du réseau. Face à ce manque de visibilité et à la difficulté d'appliquer des politiques de sécurité de manière uniforme, les organisations ont besoin d'une solution capable de contrôler l'accès, d'identifier les utilisateurs et de vérifier l'état des appareils avant de leur donner une connectivité complète.

PROBLÉMATIQUE

- Comment authentifier les utilisateurs ?
- Comment vérifier l’état et la conformité des appareils ?

OBJECTIFS

Étudier les concepts NAC

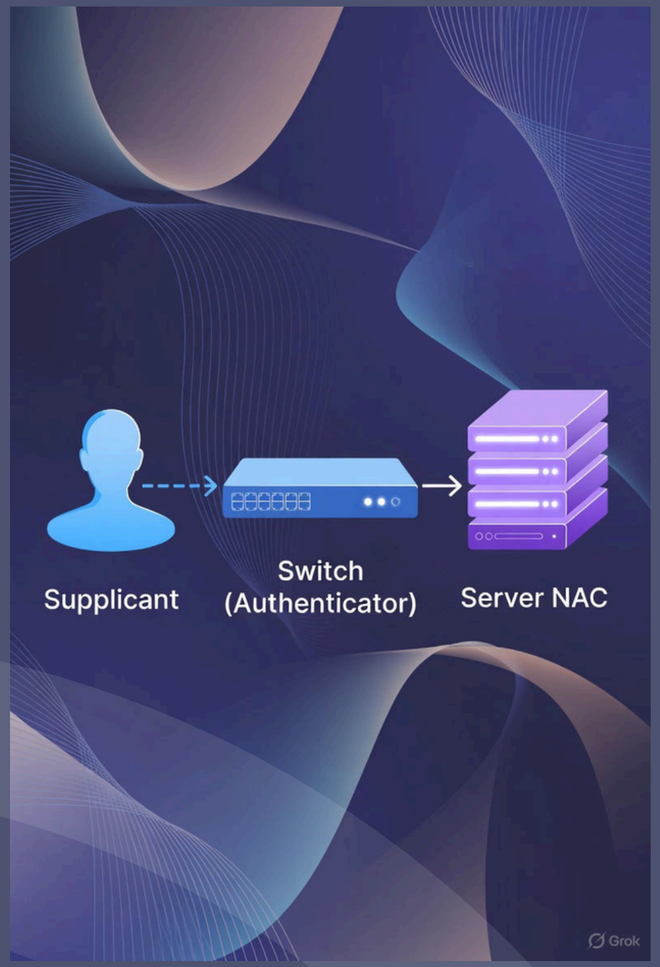
Déployer PacketFence

Intégrer Nessus

Vérifier la conformité des appareils

Tester des scénarios réels

QU'EST-CE QUE LE NAC ?



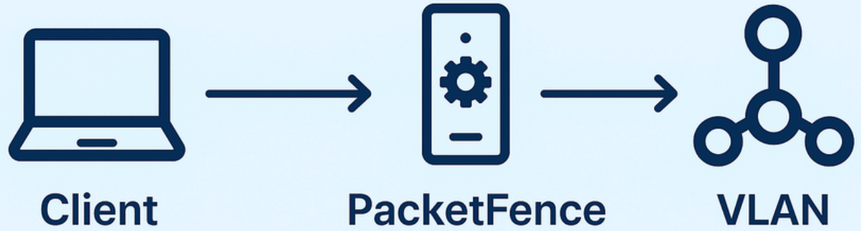
- Le NAC (Network Access Control) est une solution qui contrôle qui peut accéder au réseau.
- Il identifie les appareils et utilisateurs.
- Il vérifie qu'ils sont conformes et sécurisés avant de leur donner un accès.
- Il bloque ou isole automatiquement les appareils non conformes.

POURQUOI UTILISER NAC ?

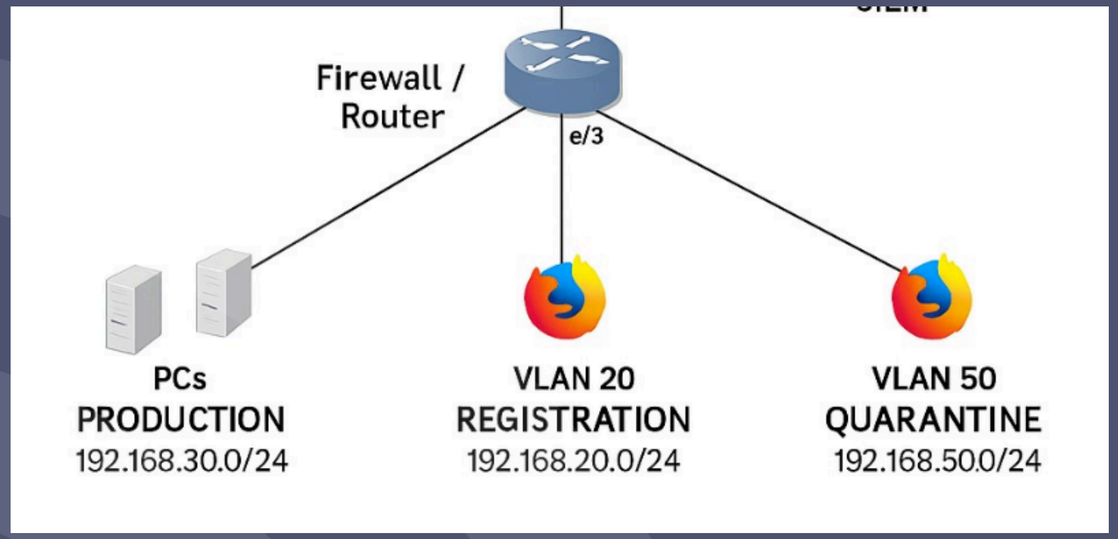
- Explosion des appareils (BYOD laptops, smartphones…).
- Risques de machines infectées ou non conformes.
- Besoin de contrôler chaque nouveau poste.
- Renforcer la sécurité interne : contrôler, surveiller, isoler.

FONCTIONNALITÉS PRINCIPALES DU NAC

- Identification (adresse MAC, 802.1X, portail captif)
- Authentification (RADIUS → utilisateurs valides)
- Évaluation de conformité (antivirus, mises à jour…)
- Segmentation dynamique (VLAN Registration / Normal / Isolation)
- Isolation automatique des appareils suspects
- Traçabilité et logs (AAA)



FONCTIONNEMENT D'UN NAC



Contenu :

- Supplicant : le client
- Authenticator : le switch
- Serveur de politique : PacketFence (RADIUS)

Processus résumé :

1. Le client se connecte au switch
2. Le switch demande l'identité
3. PacketFence vérifie & décide
4. Le switch place l'appareil dans le bon VLAN

Avantages du NAC

- **Améliore fortement la sécurité interne**
- **Empêche les connexions non autorisées**
- Évite la propagation de malware
- **Automatisation du contrôle d’accès**
- **Visibilité totale sur les appareils du réseau**

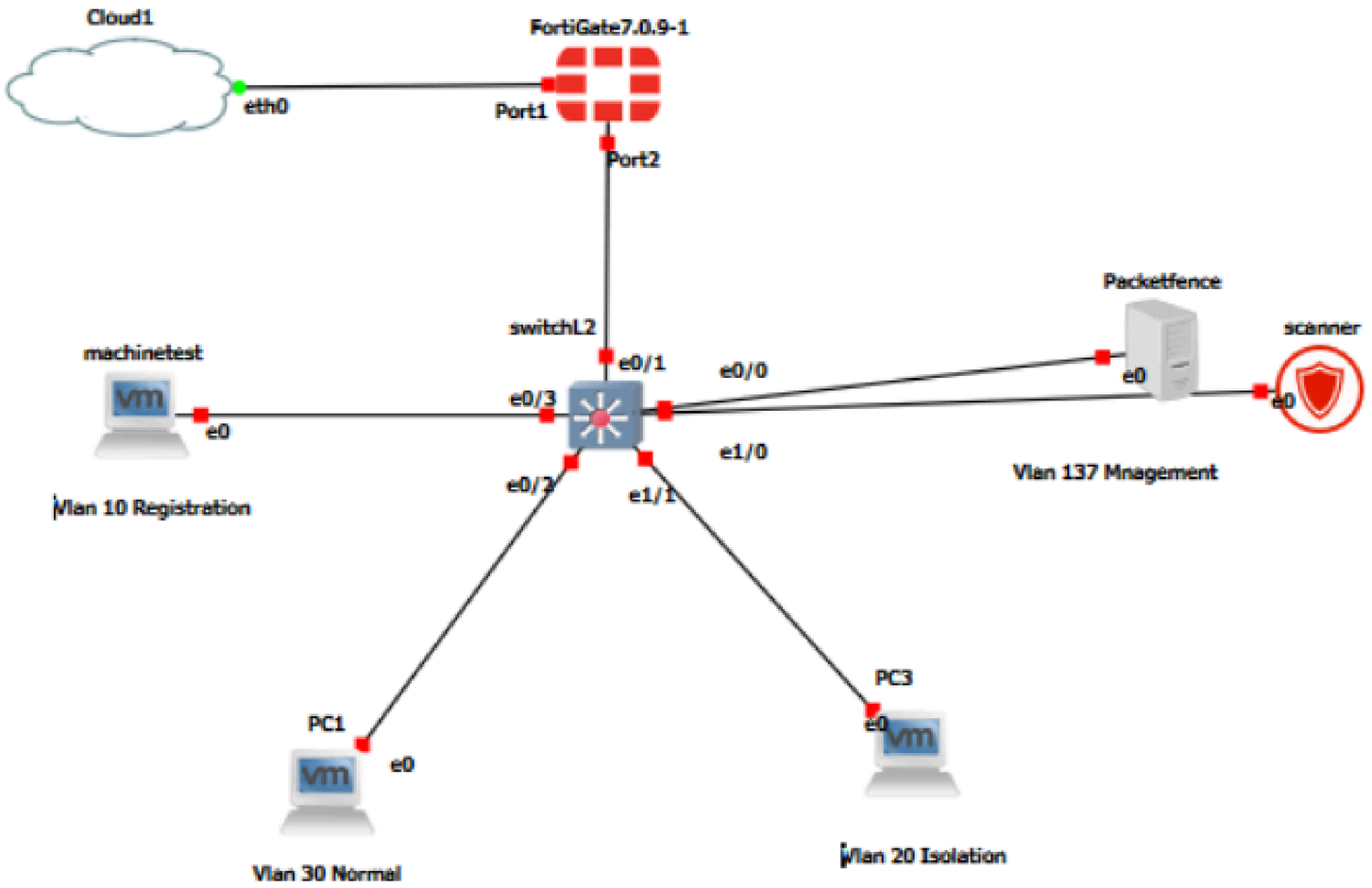
TECHNOLOGIES UTILISÉES

- Déploiement des serveurs et machines clientes
- Tests en environnement contrôlé

- Solution NAC open-source
- WPA SUPPLICANT
- Authentification & gestion des politiques
- Attribution dynamique des VLANs

- Analyse vulnérabilités
- Plugins et scans

TOPOLOGIE


Cloud1
eth0
FortiGate7.0.9-1
Port1
Port2
switchL2
e0/1
e0/3
e0/2
e1/1
e0/0
e1/0
machinetest
e0
Vlan 10 Registration
Packetfence
e0
scanner
e0
Vlan 137 Mnagement
PC1
e0
Vlan 30 Normal
PC3
e0
Vlan 20 Isolation

Principe du Time-of-Band dans PacketFence

Dans PacketFence, il existe deux modes pour contrôler et authentifier les utilisateurs sur le réseau :

In-Band

Tout le trafic réseau (data + contrôle) passe à travers PacketFence.

➡️ PacketFence devient un pont obligatoire entre les machines et le réseau.

Out-of-Band (OOB)

C’est le mode le plus utilisé dans les architectures NAC modernes.

➡️ Time-of-Band = PacketFence ne voit pas le trafic de l’utilisateur,

➡️ Il ne contrôle que le moment où il doit agir (changement de VLAN, mise en quarantaine, etc.)

Le 1er pilier de NAC :

AUTHENTIFICATION

Les Mécanismes d’Authentification Utilisés dans Notre Déploiement NAC

Server RADIUS (Intégré dans PacketFence)

- PacketFence intègre un serveur RADIUS qui centralise et traite toutes les demandes d’authentification provenant du réseau.
- **Fonctions principales**
  - **Validation de l’identité**

    Vérifie les identifiants des utilisateurs et des appareils .
  - **Interaction avec le switch via 802.1X**

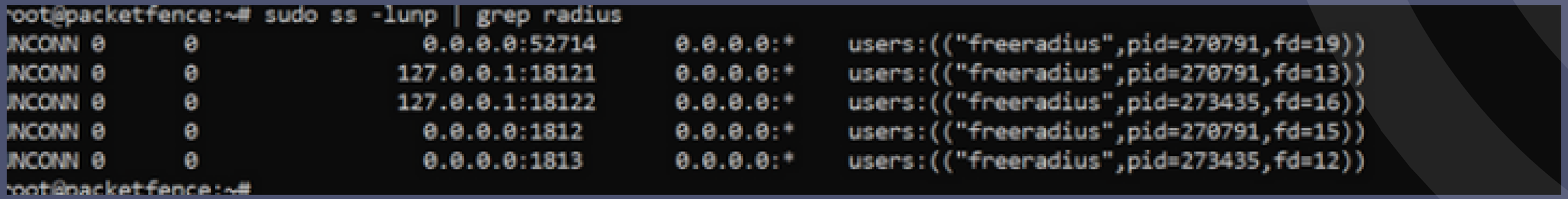
    Le switch transmet les demandes d’authentification à PacketFence en utilisant le protocole 802.1X.

Dans PacketFence, deux services RADIUS sont actifs et travaillent ensemble:

packetfence-radiusd-auth.service : s'occupe de l'authentification, c'est-à-dire qu'il vérifie l'identité des utilisateurs lorsqu'ils se connectent via 802.1X.

packetfence-radiusd-acct.service : prend le relais pour la comptabilité : il enregistre les sessions utilisateurs, la durée des connexions et d'autres informations importantes pour le suivi et la gestion du réseau.

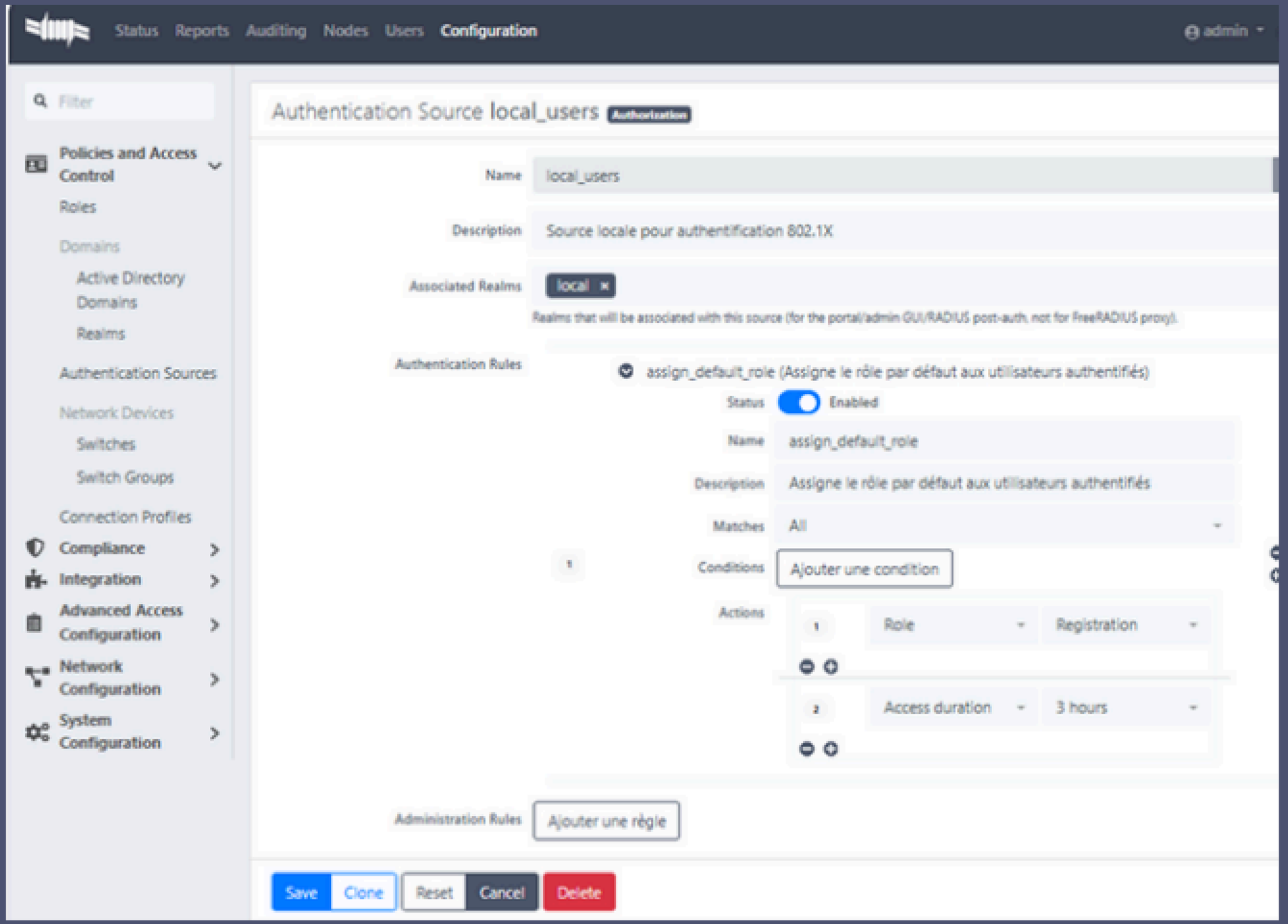
Verification de ports:



- La commande ss -lunp | grep radius confirme que les services RADIUS de Packetfence) sont bien démarrés et écoutent sur les ports standards
- **1812 = Authentification**
- **1813 = Accounting (suivi des sessions)**

Configuration de la Source d'Authentification RADIUS

- La source d'authentification est un système d'authentification autonome qui utilise une base de données locale intégrée à PacketFence pour vérifier les identités des utilisateurs lors des connexions 802.1X.
- Contrairement aux sources externes comme Active Directory ou LDAP, cette source stocke directement les credentials (noms d'utilisateur et mots de passe) dans PacketFence.


Status
Reports
Auditing
Nodes
Users
Configuration
admin
Filter
Policies and Access Control
Roles
Domains
Active Directory Domains
Realms
Authentication Sources
Network Devices
Switches
Switch Groups
Connection Profiles
Compliance
Integration
Advanced Access Configuration
Network Configuration
System Configuration
Authentication Source local_users
Authorization
Name
local_users
Description
Source locale pour authentification 802.1X
Associated Realms
local
Realms that will be associated with this source (for the portal/admin GUI/RADIUS post-auth, not for FreeRADIUS proxy).
Authentication Rules
assign_default_role (Assigne le rôle par défaut aux utilisateurs authentifiés)
Status
Enabled
Name
assign_default_role
Description
Assigne le rôle par défaut aux utilisateurs authentifiés
Matches
All
Conditions
Ajouter une condition
Actions
Role
Registration
Access duration
3 hours
Administration Rules
Ajouter une règle
Save
Clone
Reset
Cancel
Delete

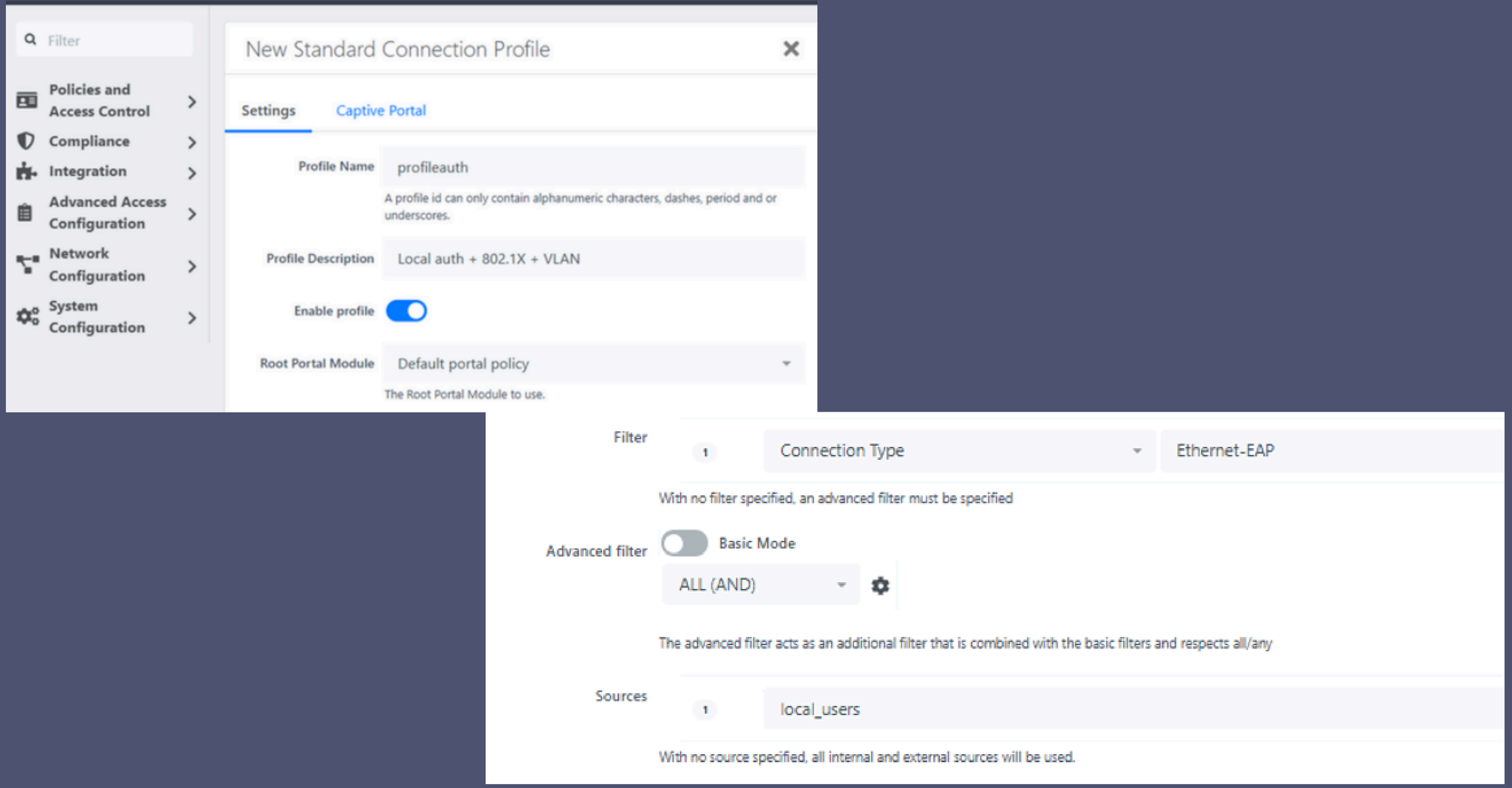
Profil de Connexion "profileauth"

- Un Profil de Connexion dans PacketFence est un ensemble de règles et de paramètres qui déterminent comment un équipement réseau (Switch, AP Wi-Fi, etc.) doit être géré lorsqu'il envoie une tentative d'authentification.
- Il indique à PacketFence quelle méthode d'authentification utiliser, quelle source d'utilisateurs consulter (Base locale, LDAP, RADIUS, AD…), et quelles actions appliquer une fois l'utilisateur reconnu (VLAN, rôle, accès, restrictions…)

- Le profil de connexion indique à PacketFence que :

il doit gérer les connexions Ethernet avec EAP/802.1X, provenant du switch L2

- il doit authentifier les utilisateurs uniquement via la base d’utilisateurs locaux


Filter
Policies and Access Control
Compliance
Integration
Advanced Access Configuration
Network Configuration
System Configuration
New Standard Connection Profile
Settings
Captive Portal
Profile Name
profileauth
A profile id can only contain alphanumeric characters, dashes, period and or underscores.
Profile Description
Local auth + 802.1X + VLAN
Enable profile
Root Portal Module
Default portal policy
The Root Portal Module to use.
Filter
1
Connection Type
Ethernet-EAP
With no filter specified, an advanced filter must be specified
Advanced filter
Basic Mode
ALL (AND)
The advanced filter acts as an additional filter that is combined with the basic filters and respects all/any
Sources
1
local_users
With no source specified, all internal and external sources will be used.

Profil EAP :

- Le profil EAP définit la manière dont le serveur RADIUS négocie et échange les informations d'authentification avec les clients 802.1X, en précisant la méthode EAP à utiliser (ex. PEAP) et le type d'authentification interne (ex. MSCHAPv2).

Les méthodes d’authentification utilisées avec 802.1X

PEAP (Protected EAP)

Crée un tunnel sécurisé entre l’utilisateur (PC) et le serveur d’authentification (PacketFence).

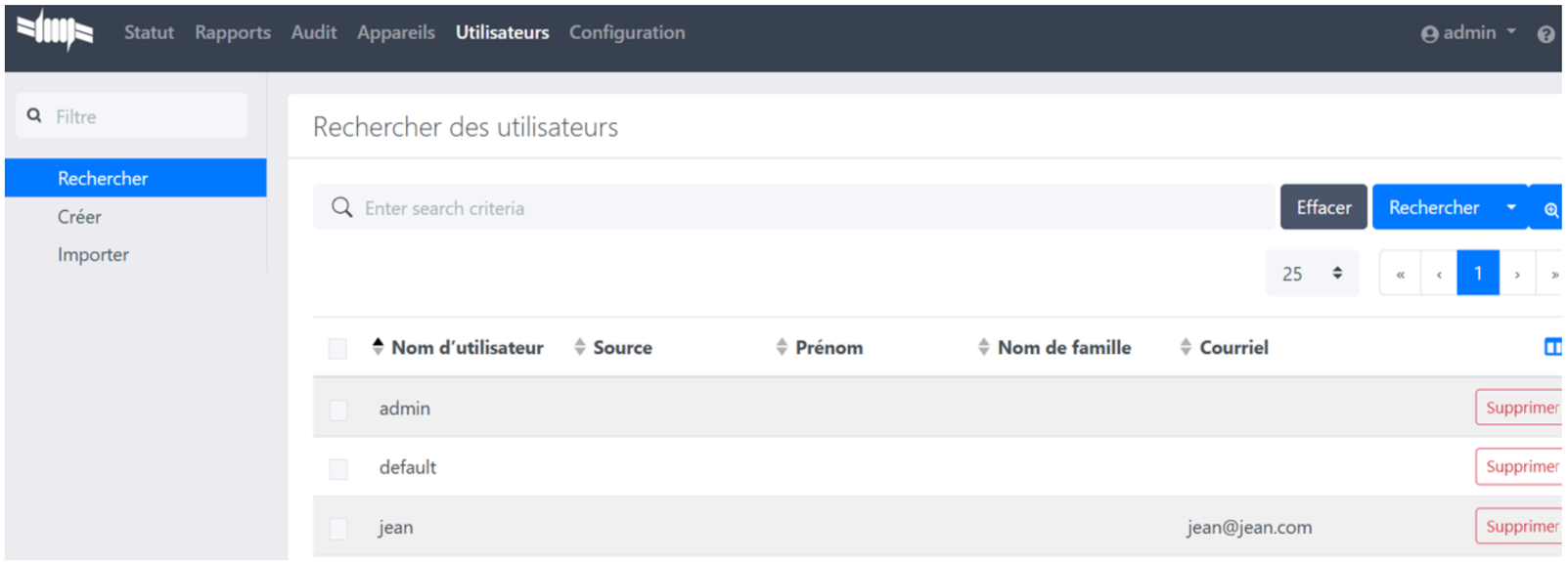
MSCHAPv2

MSCHAPv2 est le protocole utilisé à l’intérieur de PEAP pour authentifier les utilisateurs de manière sécurisée sans envoyer le mot de passe en clair

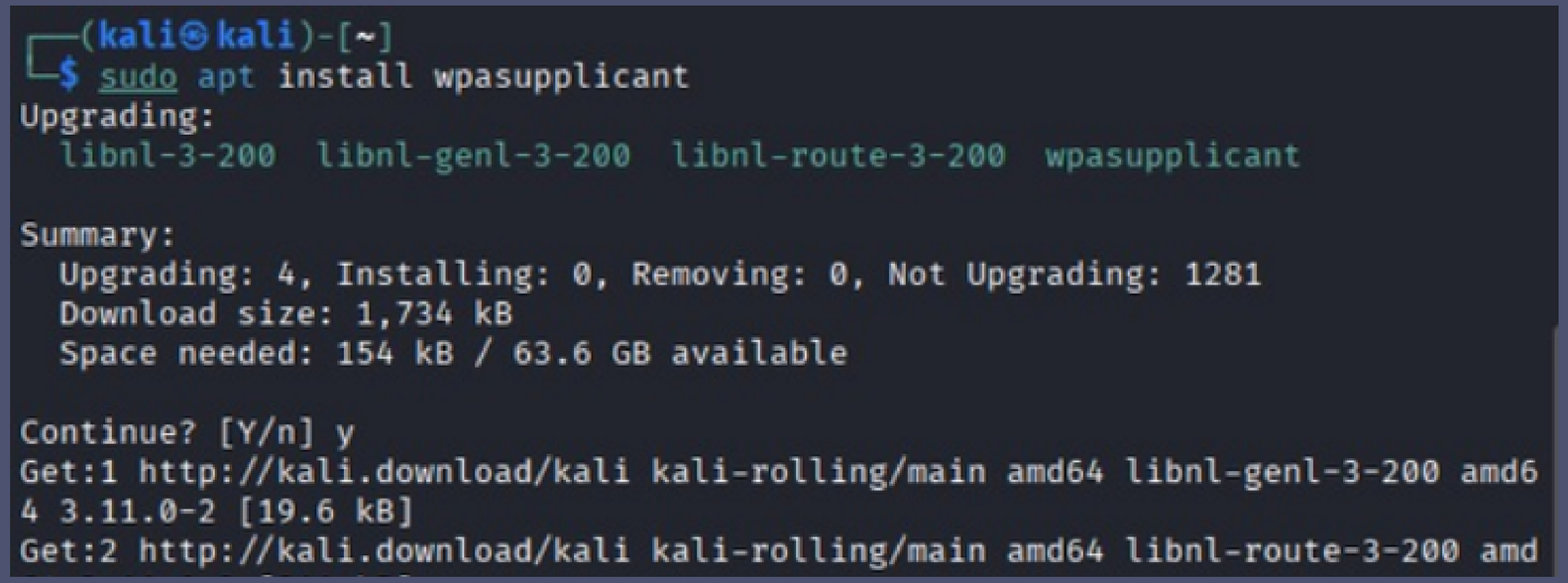
Tests d'authentification:

Cas 1 – Utilisateur Jean (présent en base)

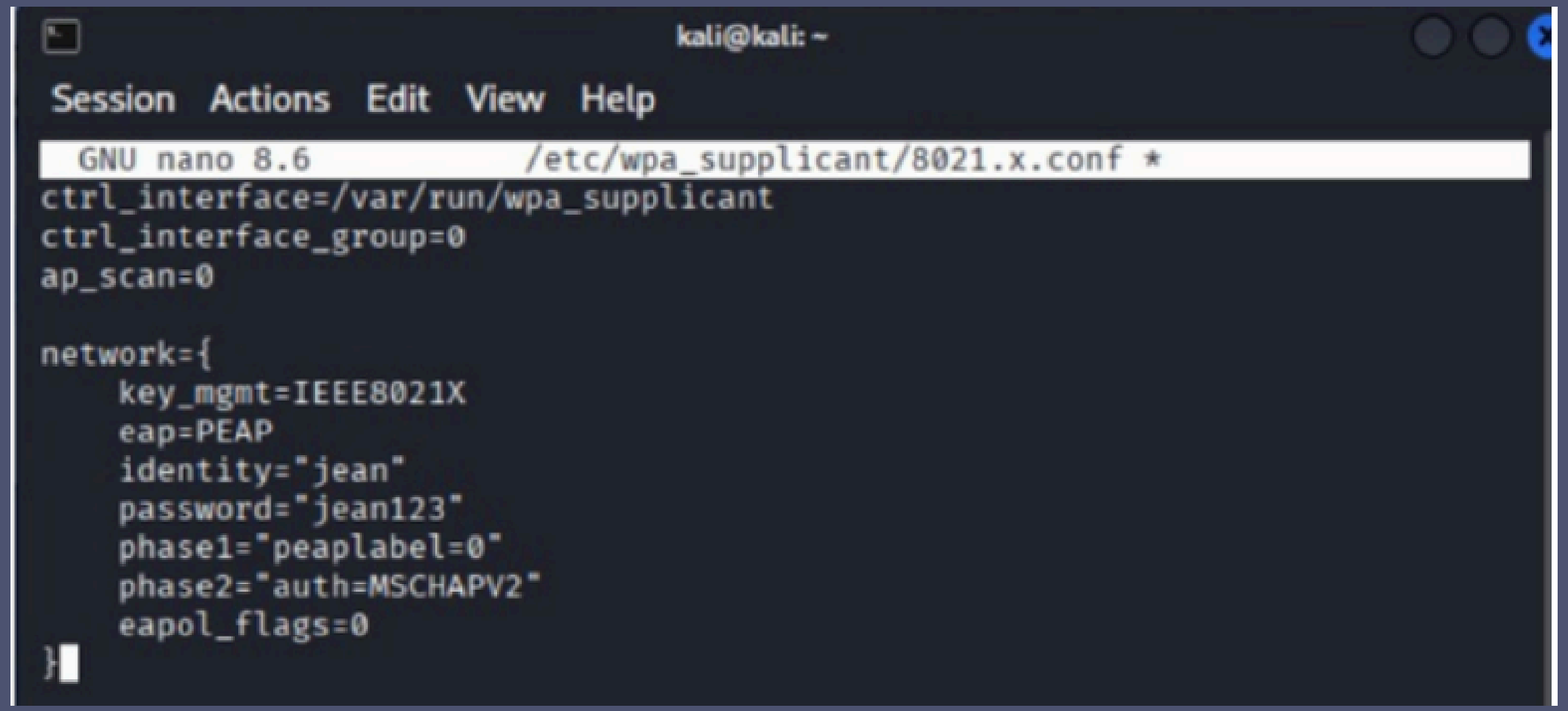
L'utilisateur Jean est présent dans la base de données locale de PacketFence. Lorsqu'il se connecte au port configuré en 802.1X, le client Kali envoie ses identifiants via EAP PEAP. PacketFence valide les identifiants et renvoie un Access-Accept. Le switch place alors le port en état Authorized



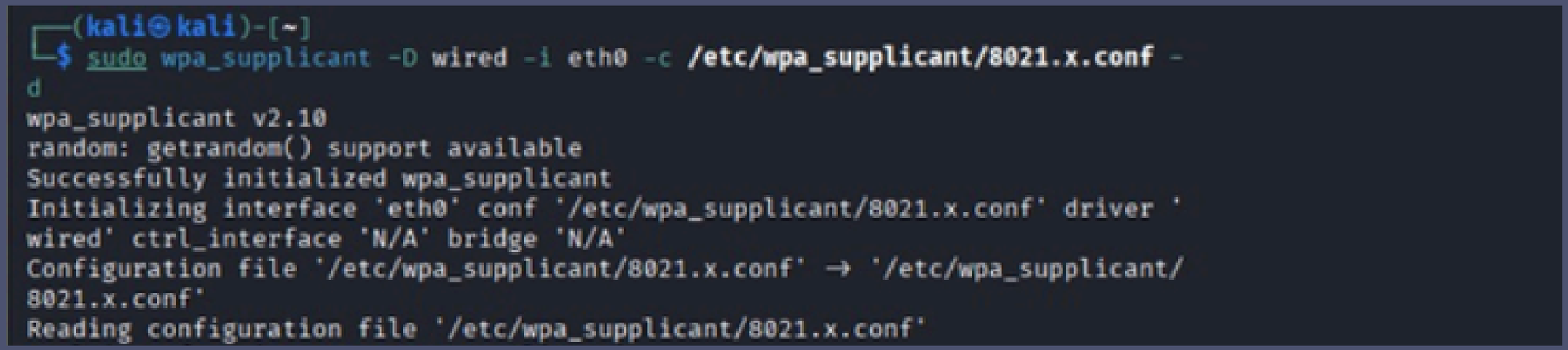
Pour commencer, nous avons installé l'outil wpa_supplicant en utilisant la commande « sudo apt install wpa-supplicant ». Cette installation est indispensable, car wpa_supplicant est le client officiel permettant à une machine Linux d'effectuer une authentification 802.1X sur un réseau filaire.



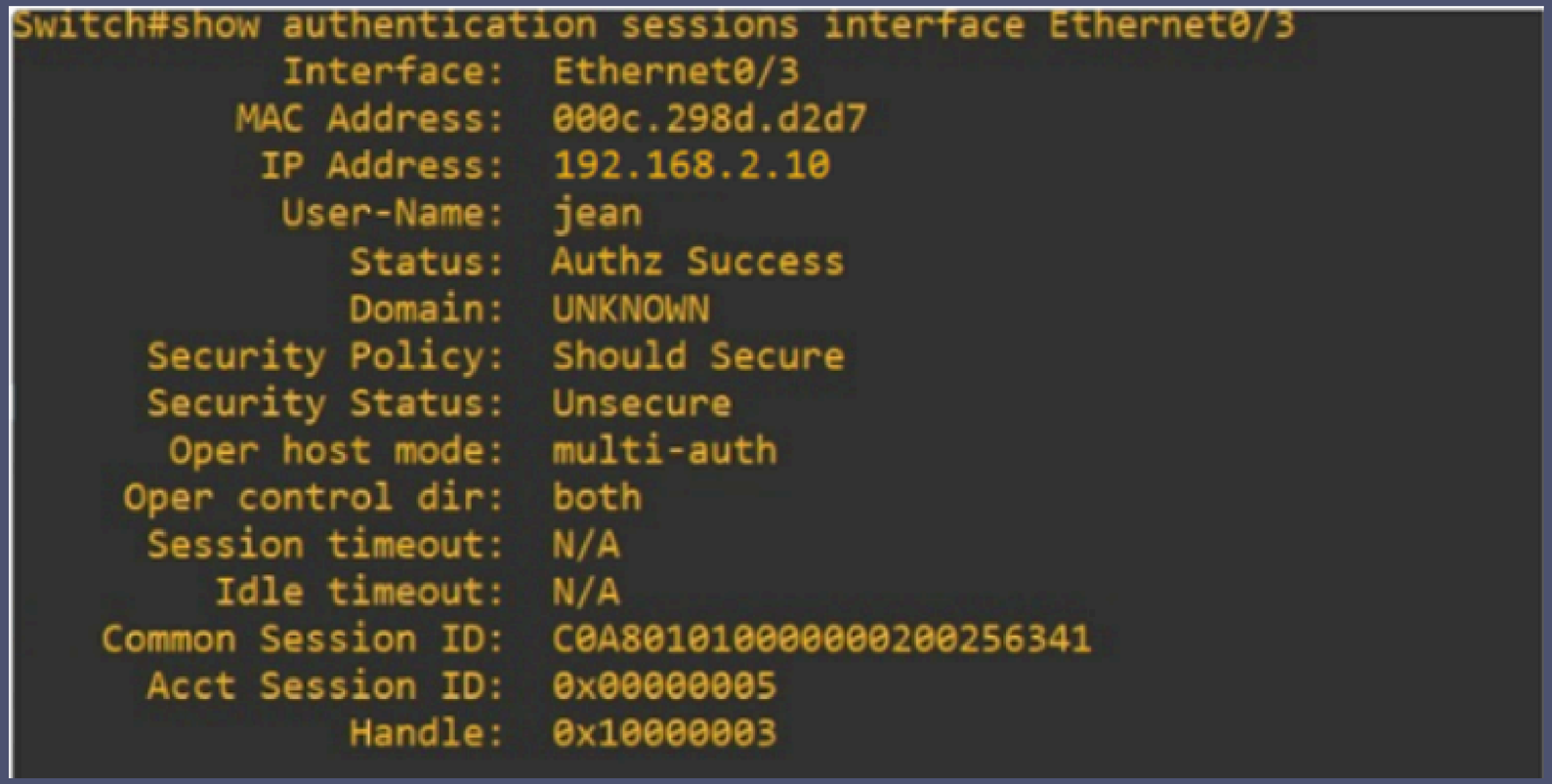
Après l’installation, nous avons configuré un fichier personnalisé pour wpa_supplicant contenant les paramètres d’authentification 802.1X. Nous avons activé key_mgmt=IEEE8021X pour l’EAPOL sur Ethernet, choisi PEAP comme méthode EAP et MSCHAPv2 pour l’authentification interne.



Une fois le fichier de configuration prêt, nous avons lancé l'authentification 802.1X en exécutant la commande « sudo wpa_supplicant -D wired -i eth0 -c /etc/wpa_supplicant/wissong.conf -d ». Cette commande permet au poste Kali de s'authentifier en EAP/PEAP via l'interface eth0, en utilisant l'identité « jean ».



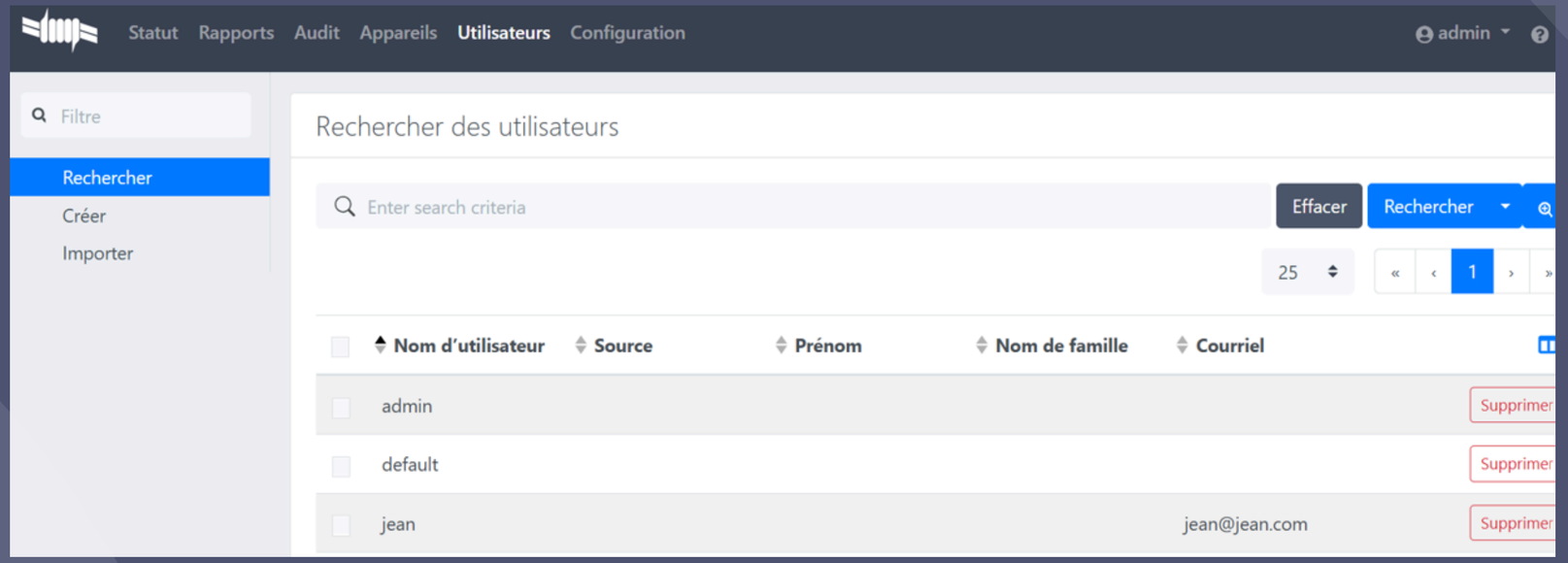
nous avons vérifié l'état du port sur le switch à l'aide de la commande « show authentication sessions interface ». Le switch affiche alors l'adresse MAC de la machine, l'utilisateur authentifié « jean » et l'adresse IP obtenue dans le VLAN registration.



Cas 2 – Utilisateur Marie (absent de la base)

Nous avons configuré wpa_supplicant dans la même machine Kali avec l’identité « Marie » et le mot de passe « Marie123 » en PEAP/MSCHAPv2. Comme Marie n’existe pas dans la base PacketFence, l’authentification échoue et wpa_supplicant affiche un message de rejet.

L’utilisateur Marie ne figure pas dans la base de données. Lorsque Kali tente de s’authentifier avec son identité, PacketFence renvoie un Access-Reject. Le switch marque donc la session comme Failed



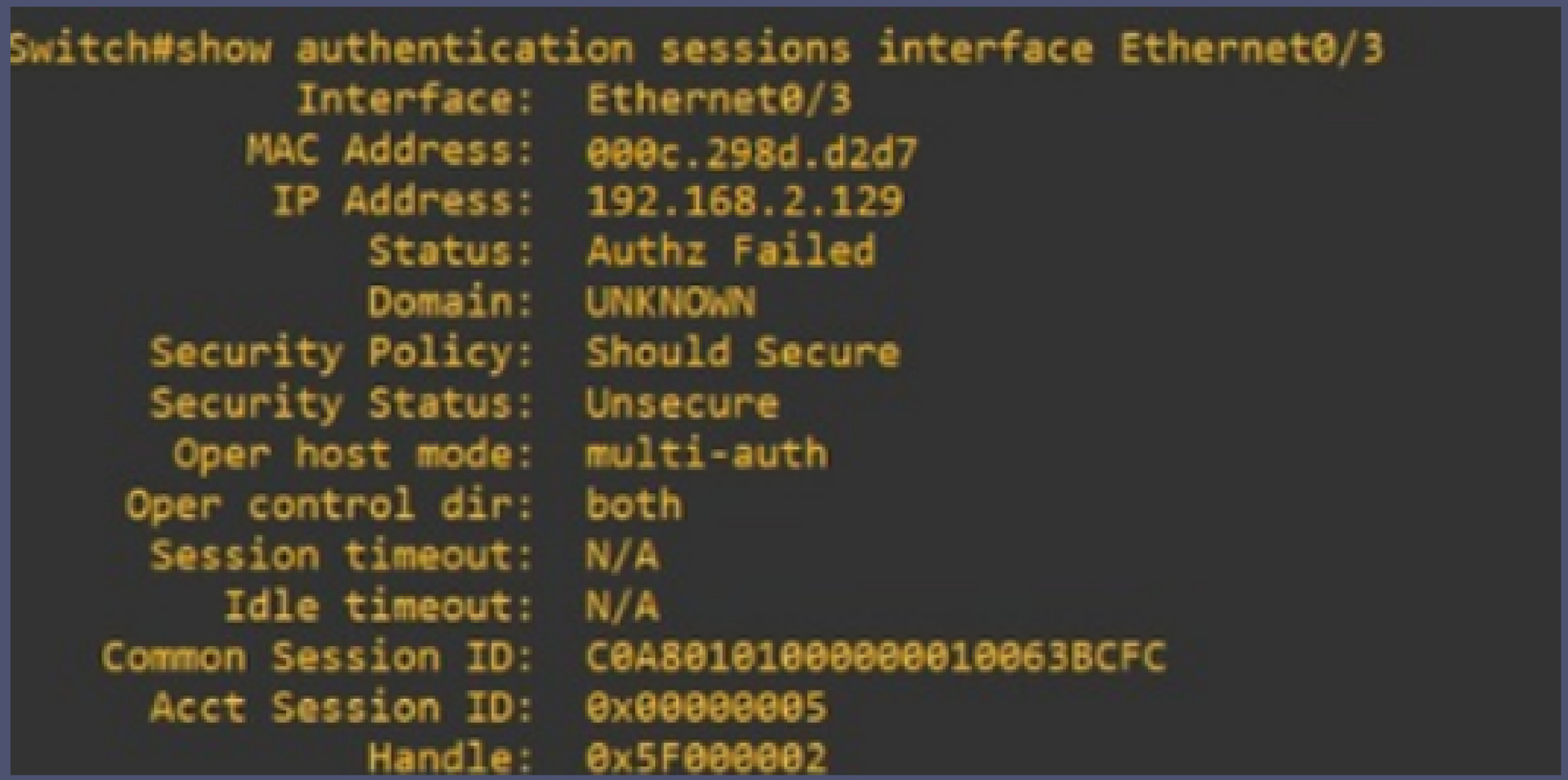
Après l’installation, nous avons configuré un fichier personnalisé pour wpa_supplicant contenant les paramètres d’authentification 802.1X. Nous avons activé key_mgmt=IEEE8021X pour l’EAPOL sur Ethernet, choisi PEAP comme méthode EAP et MSCHAPv2 pour l’authentification interne.

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0

ap_scan=0
eapol_version=1

network={
    key_mgmt=IEEE8021X
    eap=PEAP
    identity="marie"
    password="marie123"
    phase1="peapver=0"
    phase2="auth=MSCHAPV2"
    eapol_flags=0
}
```

La commande « show authentication sessions interface » montre que le switch a détecté l'adresse MAC et l'adresse IP renouvelée de la machine. Le statut est « auth failed » puisque Mary n'est pas enregistrée dans PacketFence.



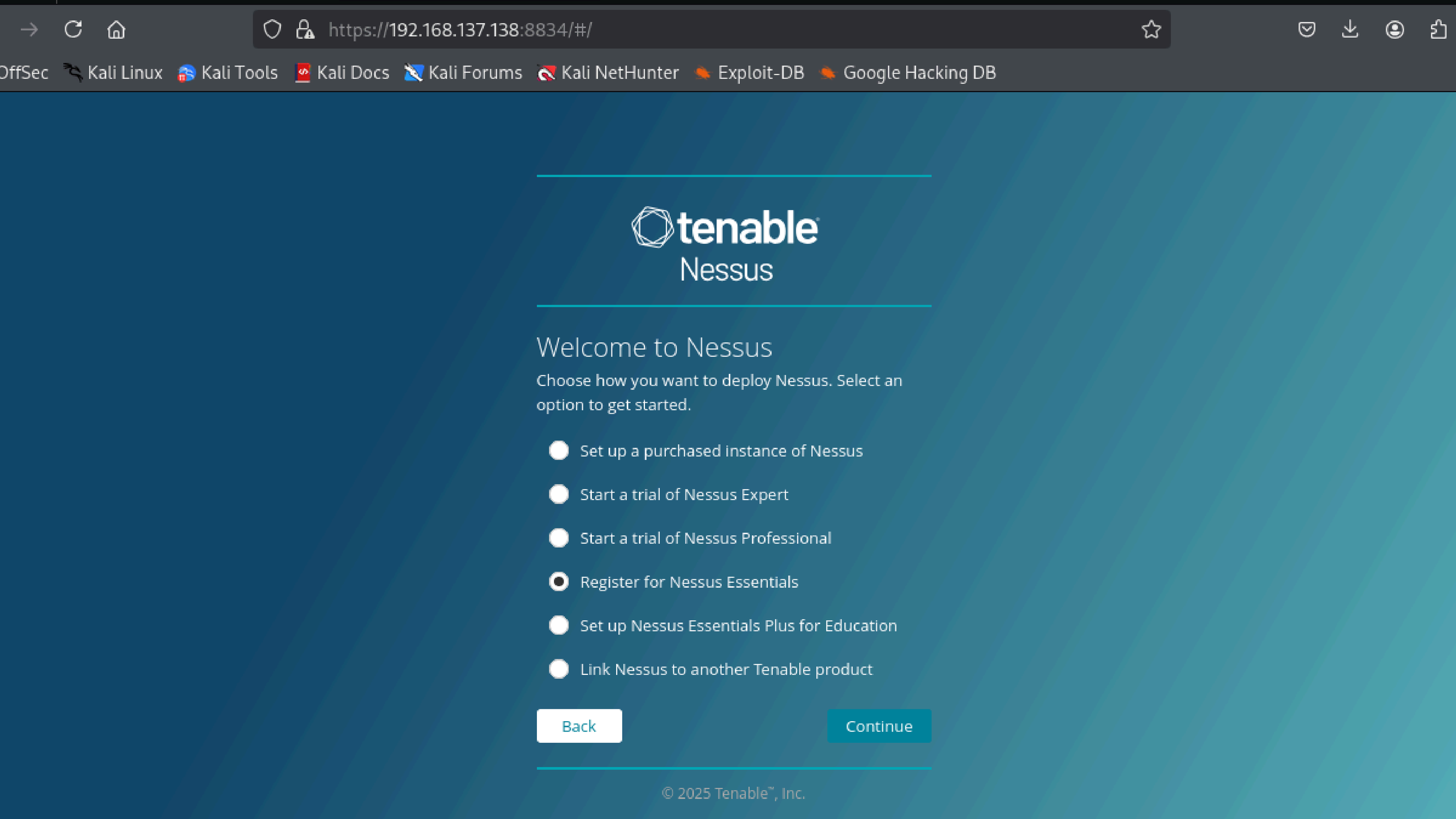
SCANNER DE VULNÉRABILITÉS

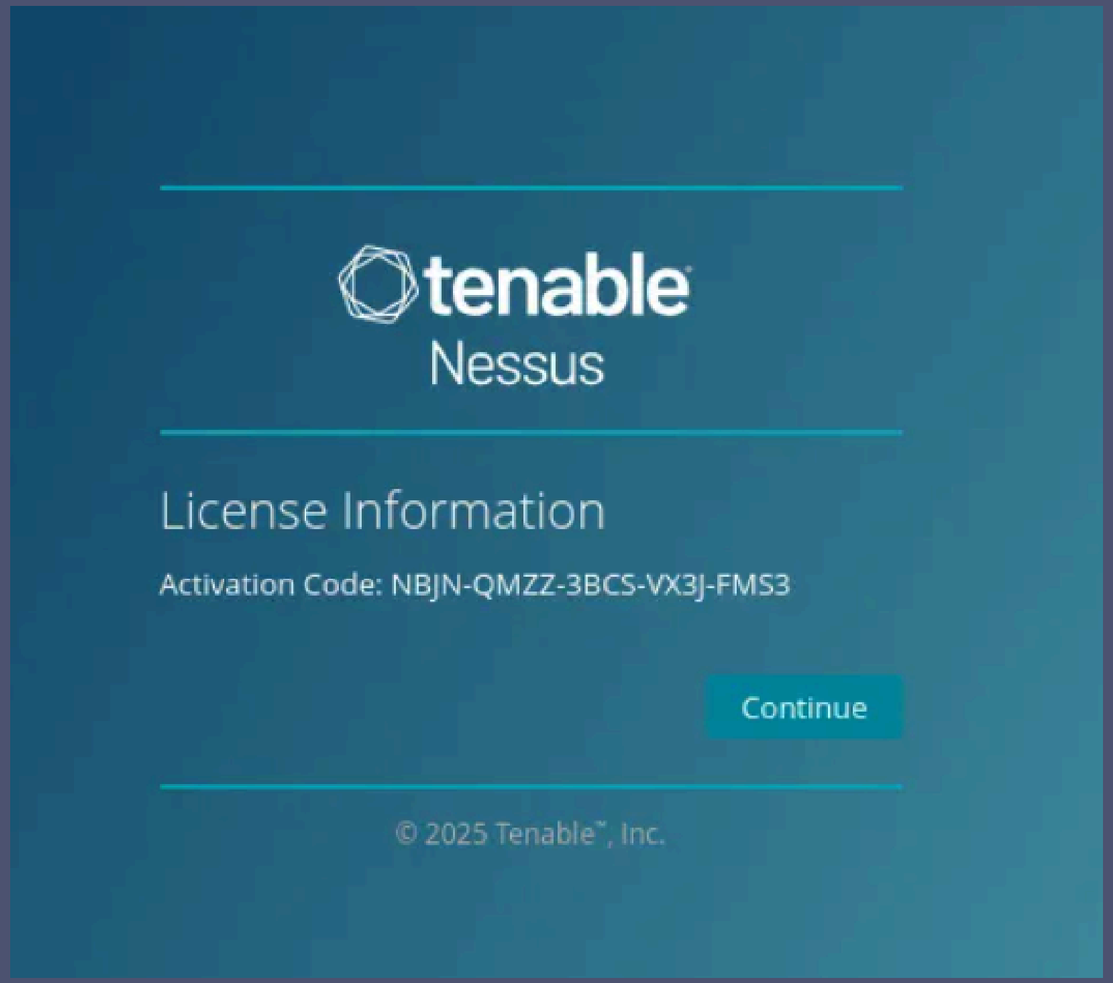
Nessus®
vulnerability scanner

SCANNER DE VULNÉRABILITÉS

- FAILLES DE SÉCURITÉ
- MAUVAISES CONFIGURATIONS
- PORTS OUVERTS
- SERVICES EXPOSÉS

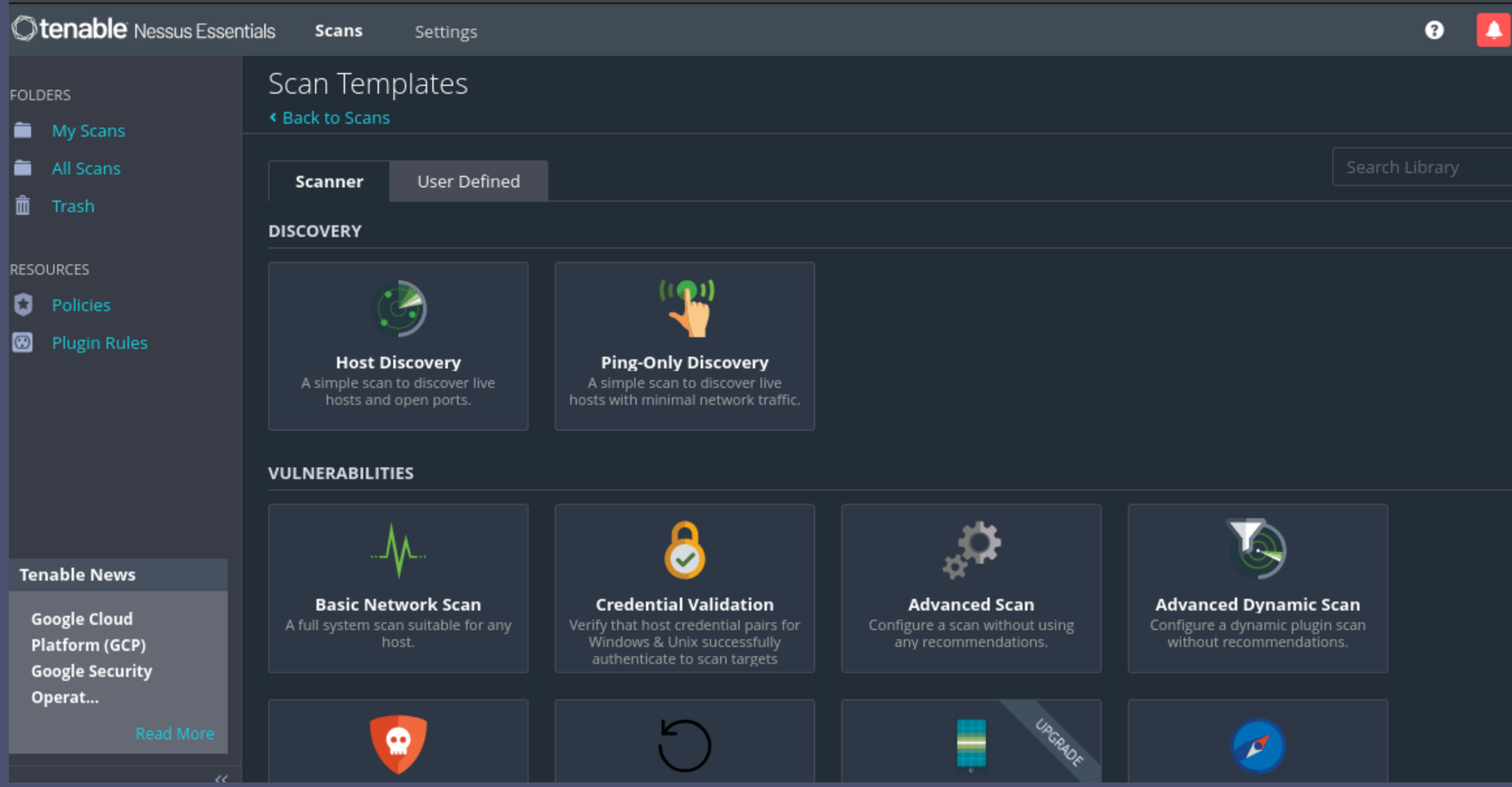
- PACKETFENCE UTILISE ENSUITE CES INFORMATIONS POUR DÉCIDER SI UN POSTE EST CONFORME OU NON. DONC EN RÉSUMÉ, NESSUS JOUE LE RÔLE DU CONTRÔLEUR DE SÉCURITÉ, ET PACKETFENCE APPLIQUE LES ACTIONS DERRIÈRE.


https://192.168.137.138:8834/#/
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
tenable
Nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select an option to get started.
Set up a purchased instance of Nessus
Start a trial of Nessus Expert
Start a trial of Nessus Professional
Register for Nessus Essentials
Set up Nessus Essentials Plus for Education
Link Nessus to another Tenable product
Back
Continue
© 2025 Tenable™, Inc.

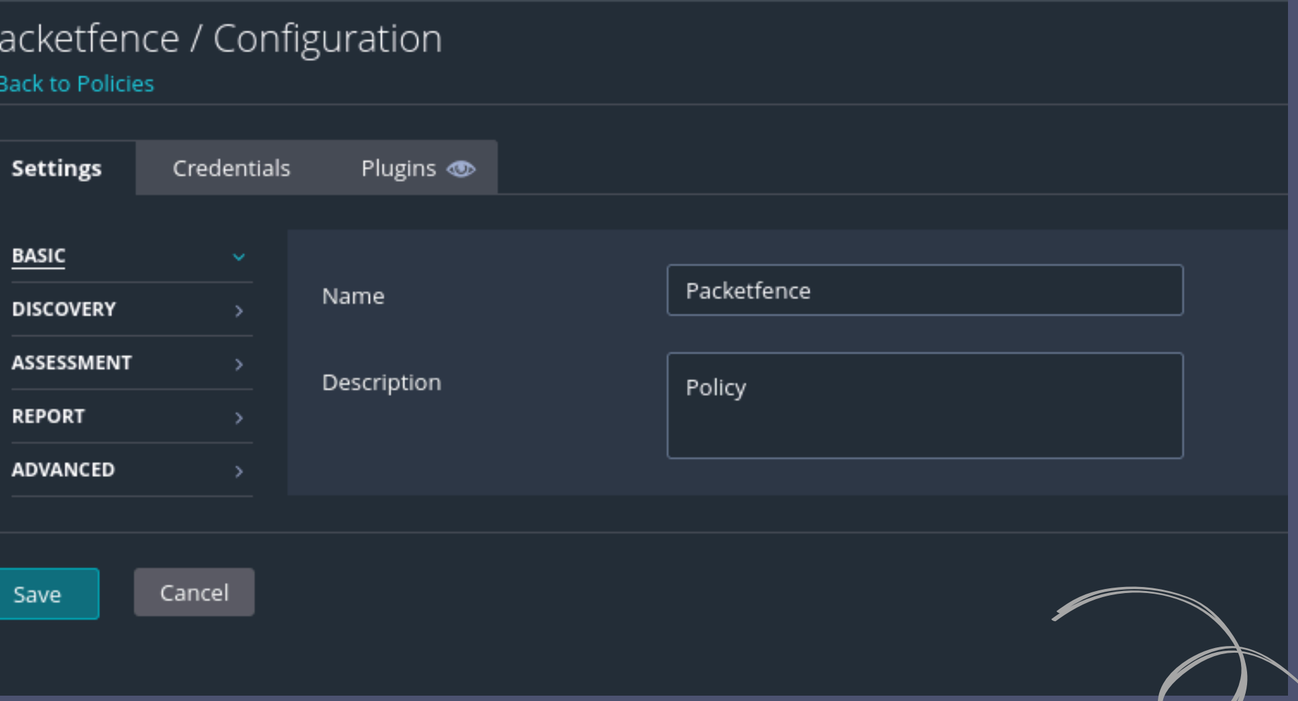

tenable
Nessus
License Information
Activation Code: NBJN-QMZZ-3BCS-VX3J-FMS3
Continue
© 2025 Tenable™, Inc.


tenable
Nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
Admin
Password *
Admin
Back
Submit
© 2025 Tenable™, Inc.

CRÉATION DE LA POLICY

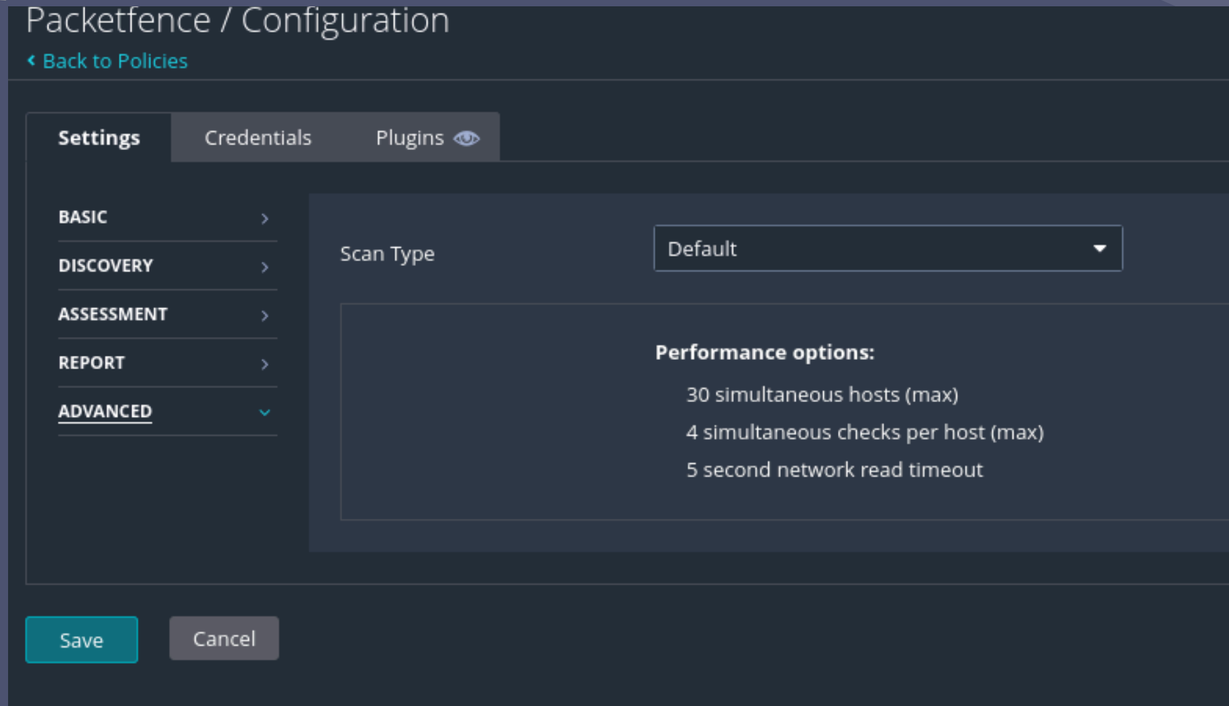


- HOST DISCOVERY, POUR DÉTECTER RAPIDEMENT LES MACHINES SUR LE RÉSEAU,
- ADVANCED SCAN, POUR UNE ANALYSE TRÈS DÉTAILLÉE,
- BASIC NETWORK SCAN, POUR UN SCAN RÉSEAU STANDARD.

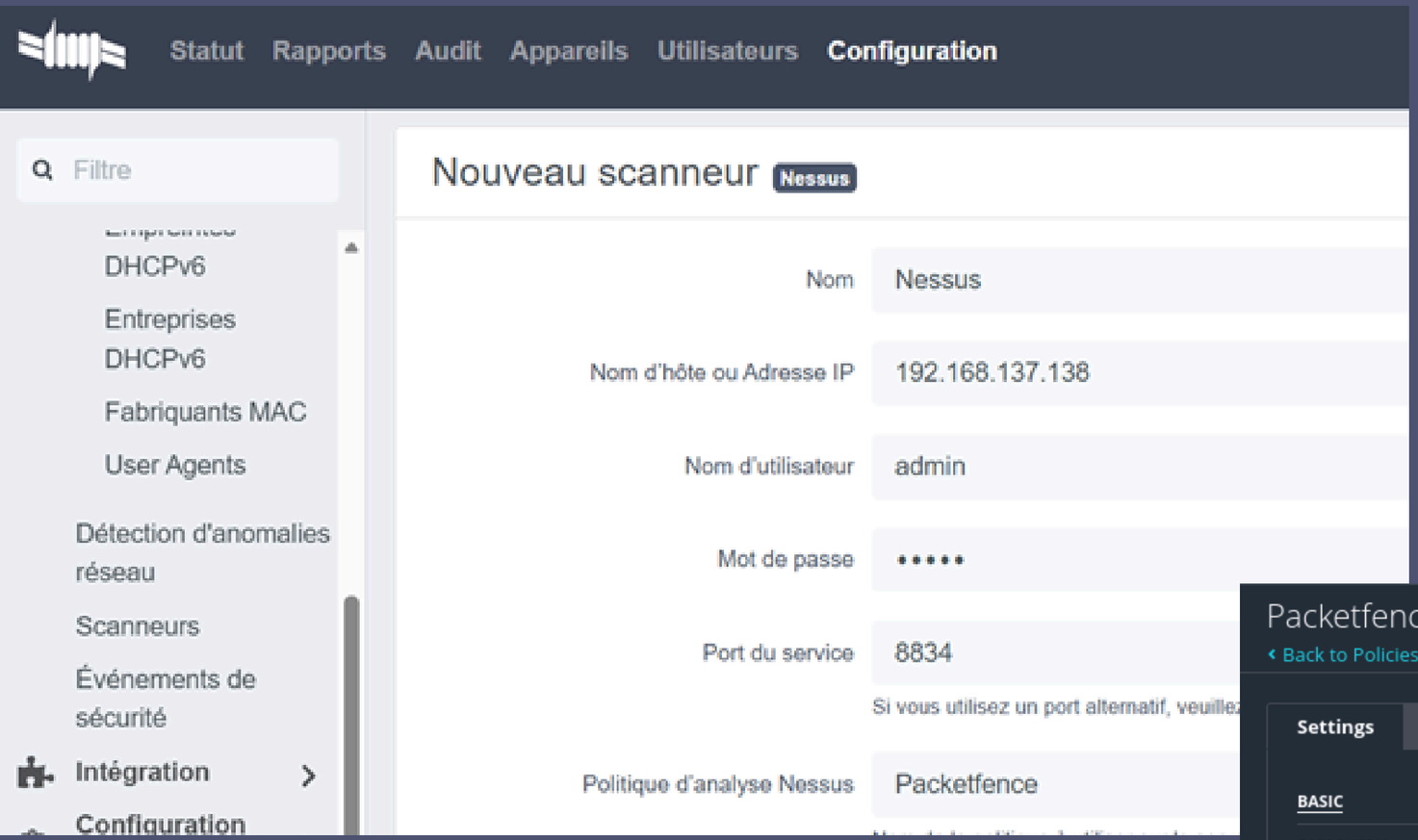


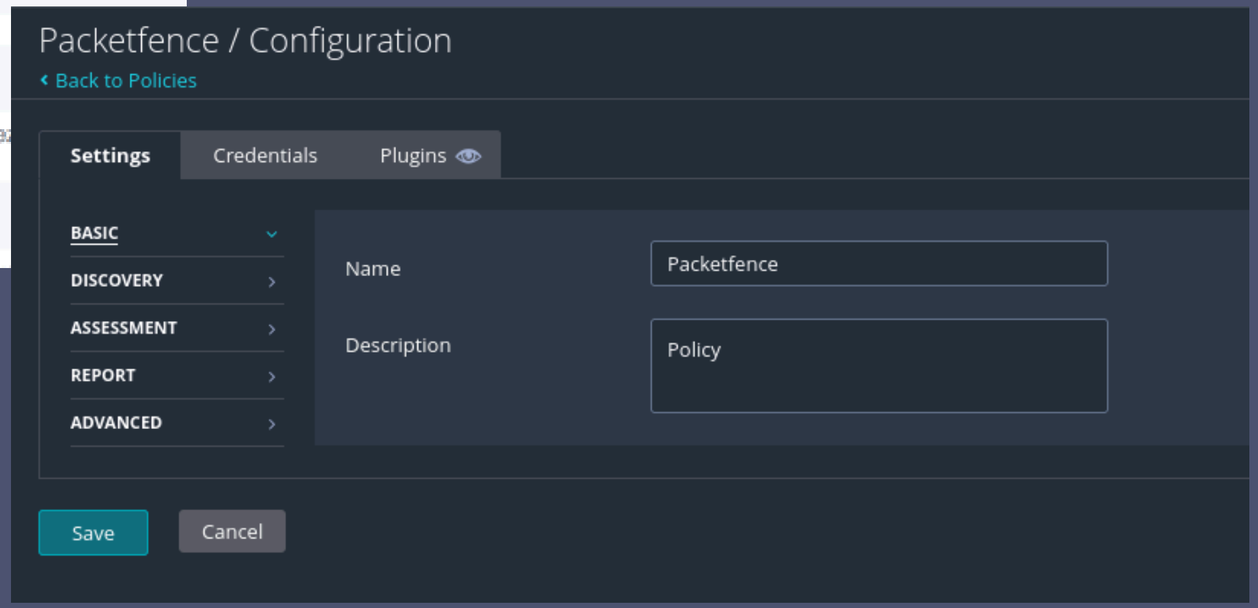
- **LA BASE DU TEST DE CONFORMITÉ**

- **SCAN TYPE DEFAULT**



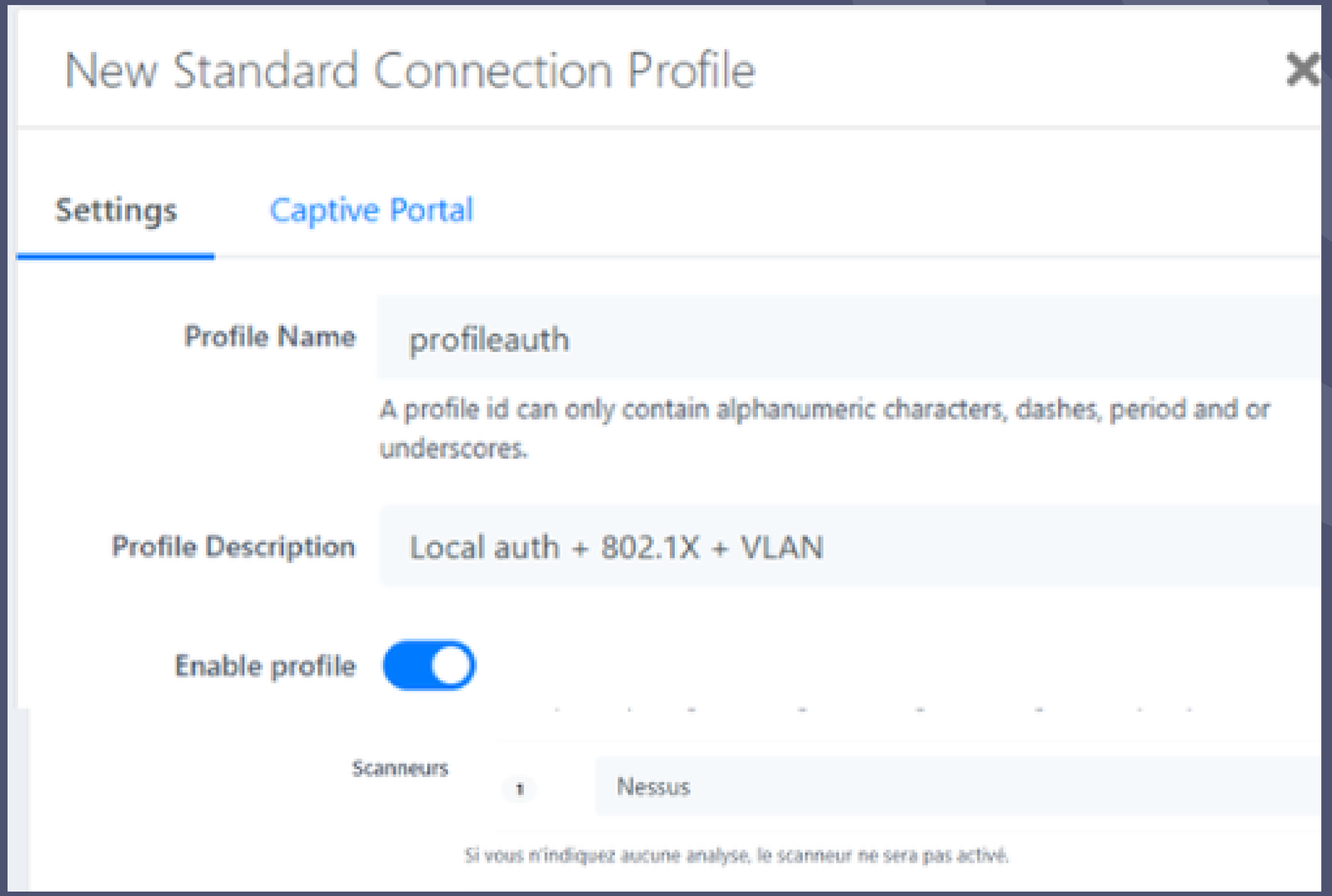
CONFIGURATION DU SCANNER DANS PACKETFENCE





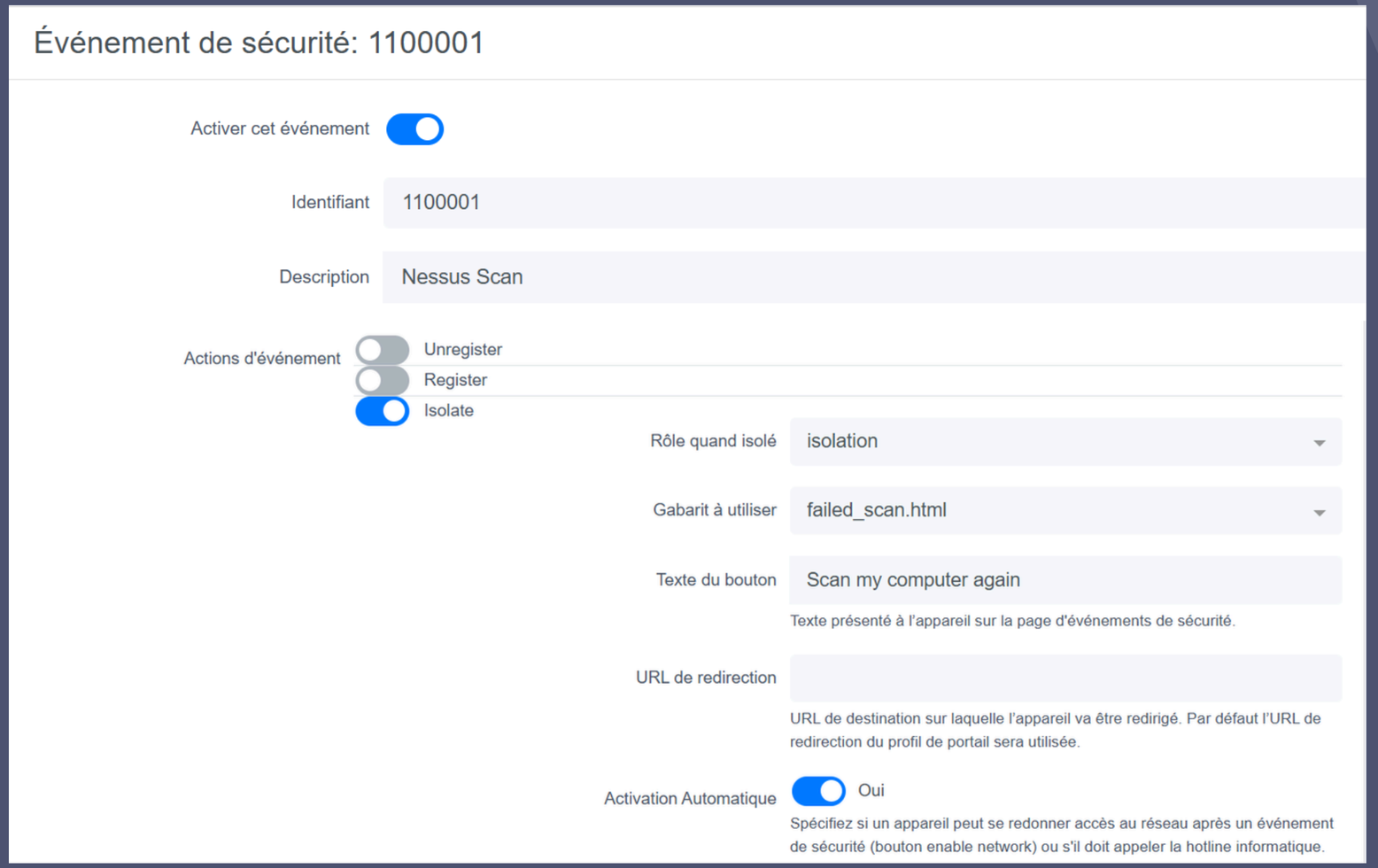
ASSOCIATION DU SCANNER AU CONNECTION PROFILE

DÈS QU'UN POSTE TENTE DE SE CONNECTER, PACKETFENCE PEUT LANCER AUTOMATIQUEMENT LE SCAN SUR CE POSTE, EN UTILISANT LA POLICY QUE NOUS AVONS DÉFINIE DANS NESSUS.

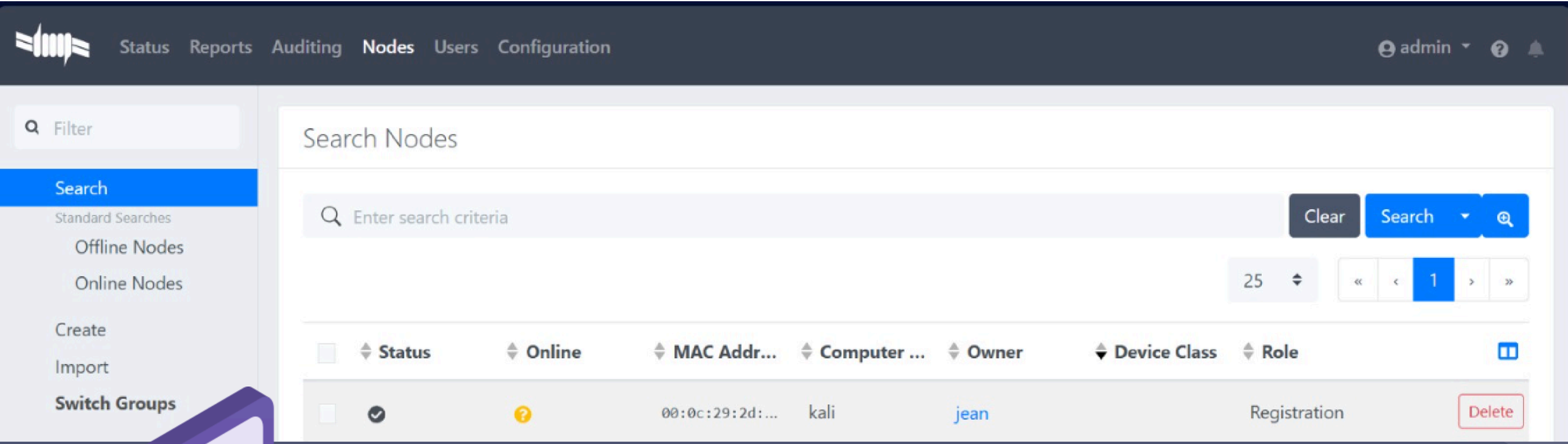


- RELIER LA DÉTECTION DU POSTE À L'ÉVALUATION DE SA CONFORMITÉ.

CRÉATION DE L'ÉVÉNEMENT DE SÉCURITÉ



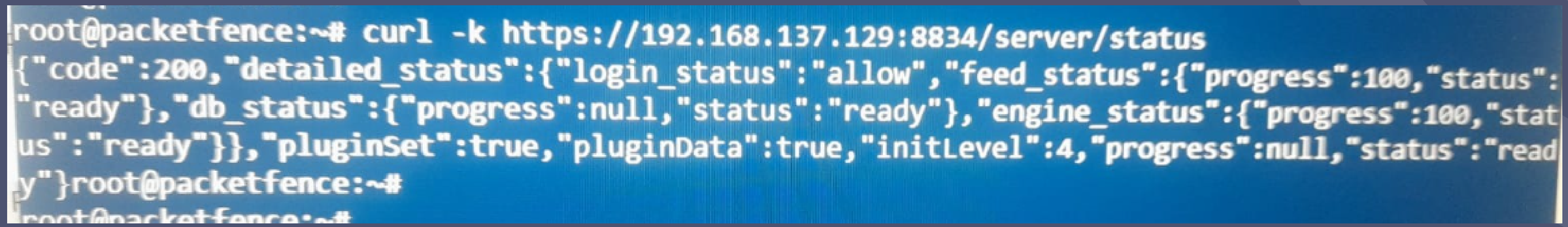
Dès qu'une vulnérabilité est détectée, PacketFence isole automatiquement le poste jusqu'à correction.



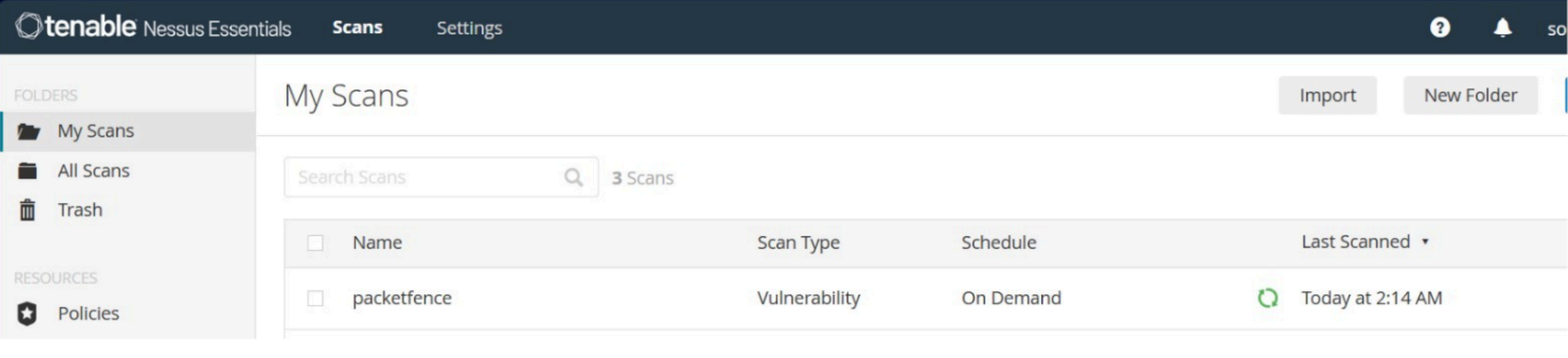
DÉTECTION DU POSTE KALI DANS PACKETFENCE

- CETTE DÉTECTION EST ESSENTIELLE POUR QUE PACKETFENCE PUISSE LANCER UN SCAN DE CONFORMITÉ PRÉCIS ET DÉCLENCHER LES ÉVÉNEMENTS DE SÉCURITÉ SI NÉCESSAIRE.

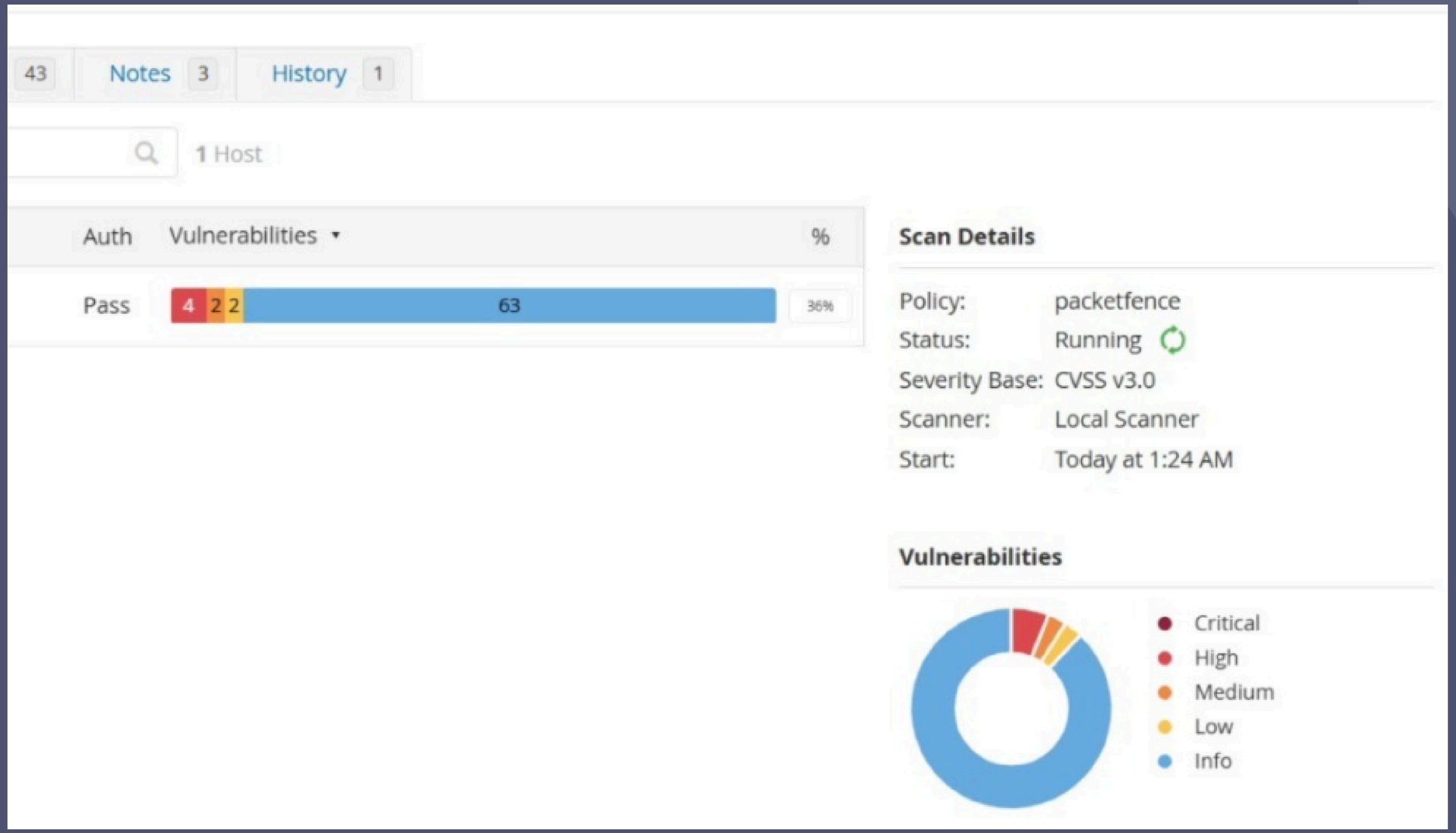
VÉRIFICATION DE LA CONNECTIVITÉ PACKETFENCE



PACKETFENCE COMMUNIQUE AVEC NESSUS VIA L'API REST SUR LE PORT SÉCURISÉ 8834. CE TEST CONFIRME QUE PACKETFENCE PEUT DEMANDER UN SCAN À NESSUS ET RECEVOIR LES RÉSULTATS. SANS CETTE CONNEXION API, LA CONFORMITÉ NE PEUT PAS FONCTIONNER.



RÉSULTATS DU SCAN SUR KALI



- NESSUS DÉTECTE DES VULNÉRABILITÉS SUR KALI
- CLASSIFICATION PAR NIVEAUX : LOW / MEDIUM / HIGH / CRITICAL

MAC 00:0c:29:2d:d7:5e

Edit | Info | Fingerbank | Timeline | IPv4 5 | IPv6 | Location | Security Events 3 | Option82

Status	Security Event	Start Date	Release Date	Ticket Ref	Notes
open	Unknown	12/03/25 12:44 am	Never		
closed	Unknown	12/03/25 12:18 am	12/03/25 12:43 am		
closed	Unknown	12/02/25 11:50 pm	12/02/25 11:58 pm		

DÉCLENCHEMENT DE L'ÉVÉNEMENT DE SÉCURITÉ

CONCLUSION