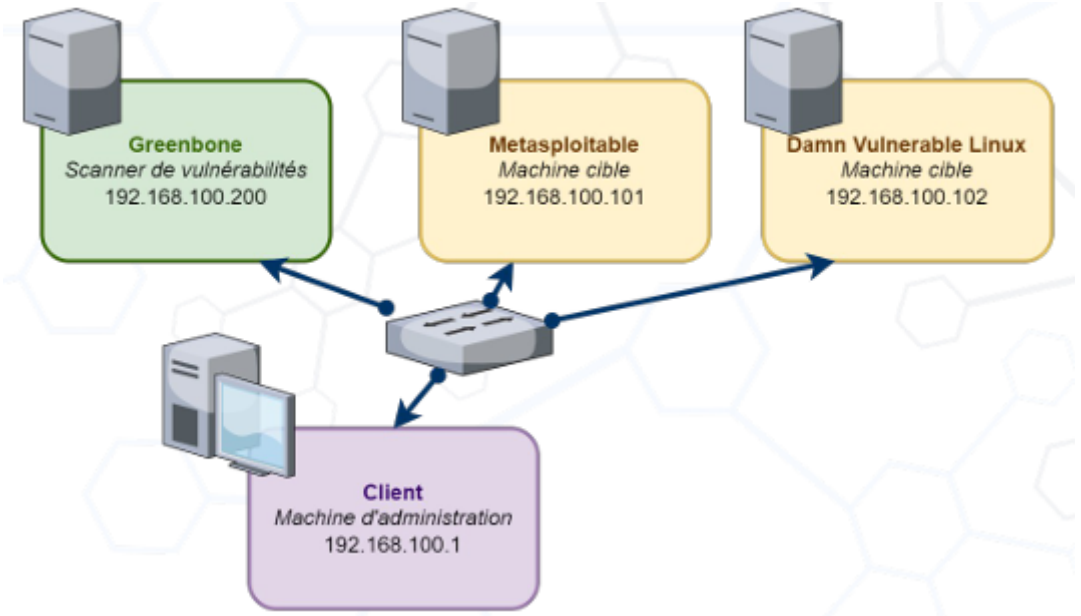
BTS 2 - Services Informatiques aux Organisations

BTS SIO SISR – Recherche de vulnérabilité : Greenbone

Tables des matières :

Topologie réseau

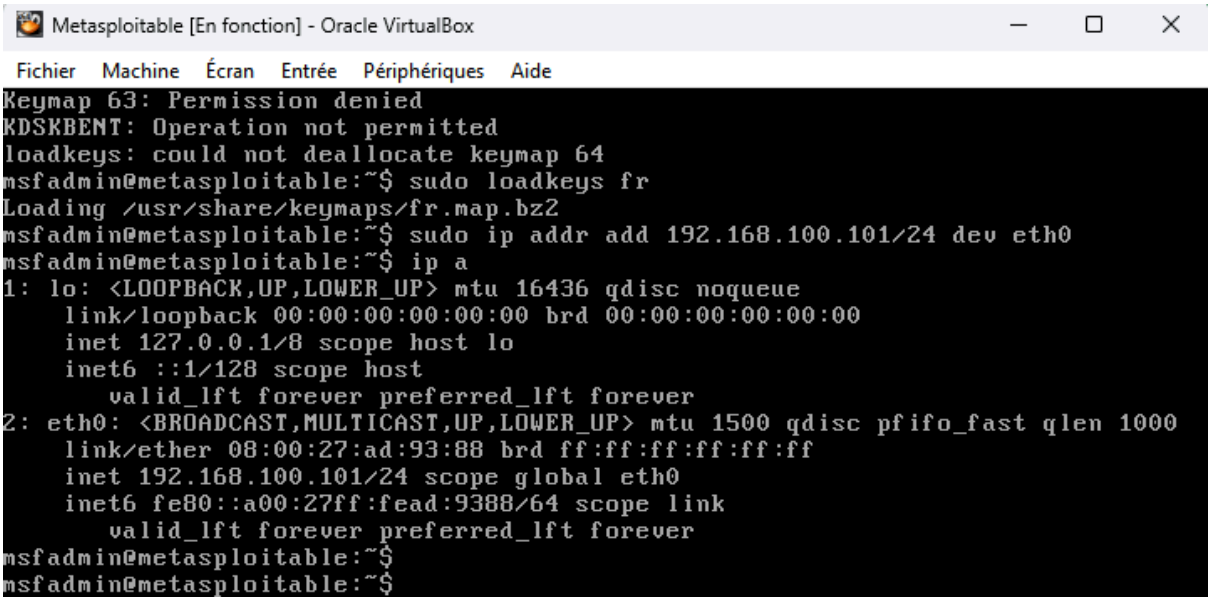


Configuration Réseau

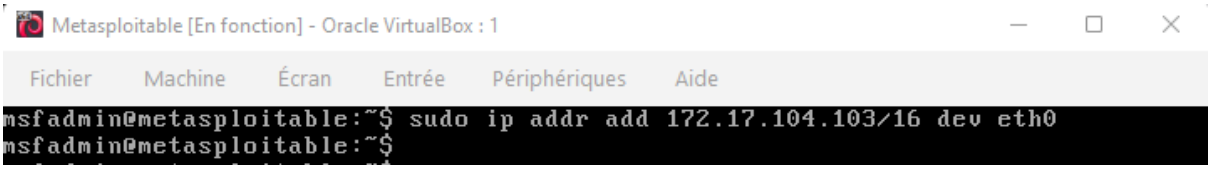
	Rôles	Type de réseau	Adresse IP	Masque	Passerelle
OpenVAS	Scanner de vulnérabilités	Réseau interne LABA et NAT	192.168.100.200 + DHCP	255.255.255.0	Aucun
Metasploitable	Machine cible vulnérable	Réseau interne LABA	192.168.100.1	255.255.255.0	Aucun
Damn Vulnerable Linux	Machine cible vulnérable	Réseau interne LABA	192.168.100.1 au lieu de 192.168.100.102 avec la VM Metasploitable éteinte pour éviter les conflits d'adressage	255.255.255.0	Aucun
Client	accès OpenVAS	Réseau local	DHCP	Automatique	Box Orange

1. Installation et configuration de Metasploitable

Arriver à cette étape je n'ai pas de vm Metasploitable donc j'ai du télécharger une VM Metasploitable: 2 ~ VulnHub.

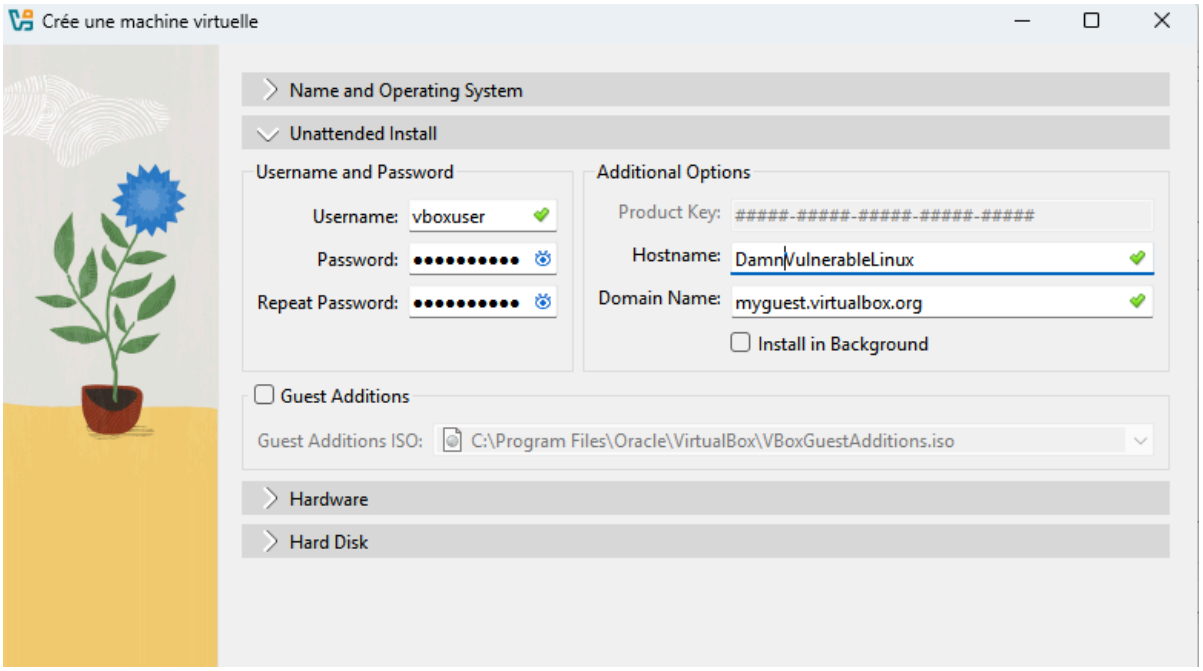


Configuration de l'adresse IP de la machine cible Metasploitable pour permettre le scan réseau avec Greenbone.

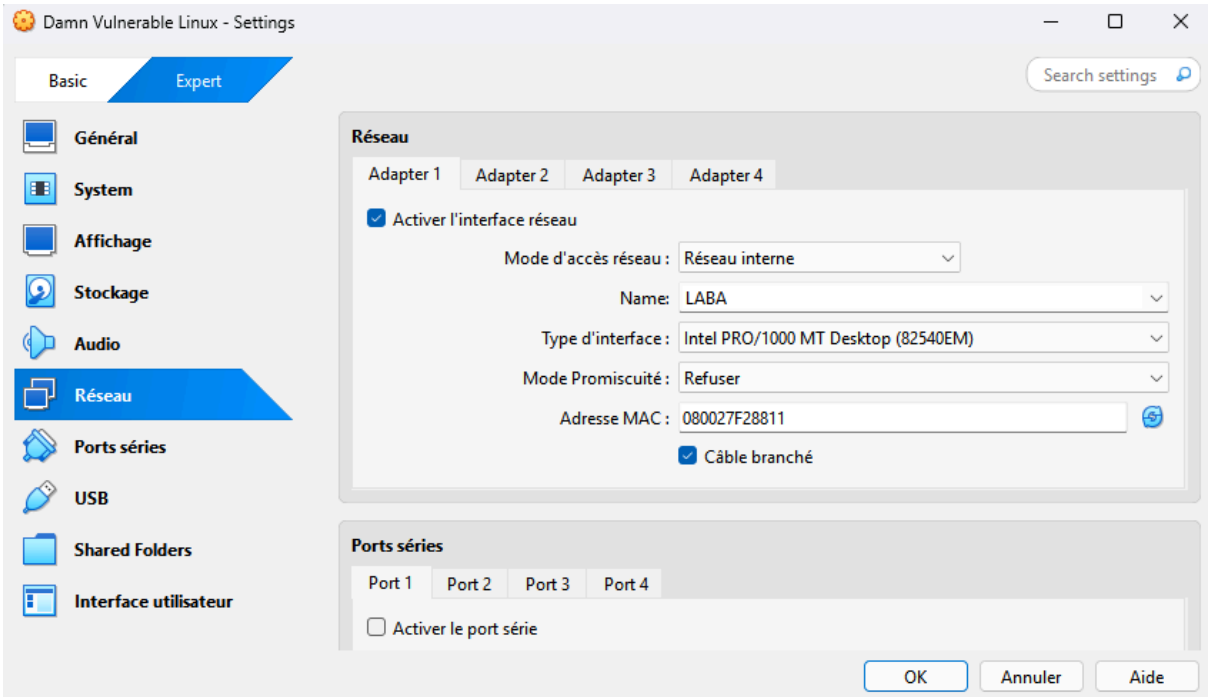


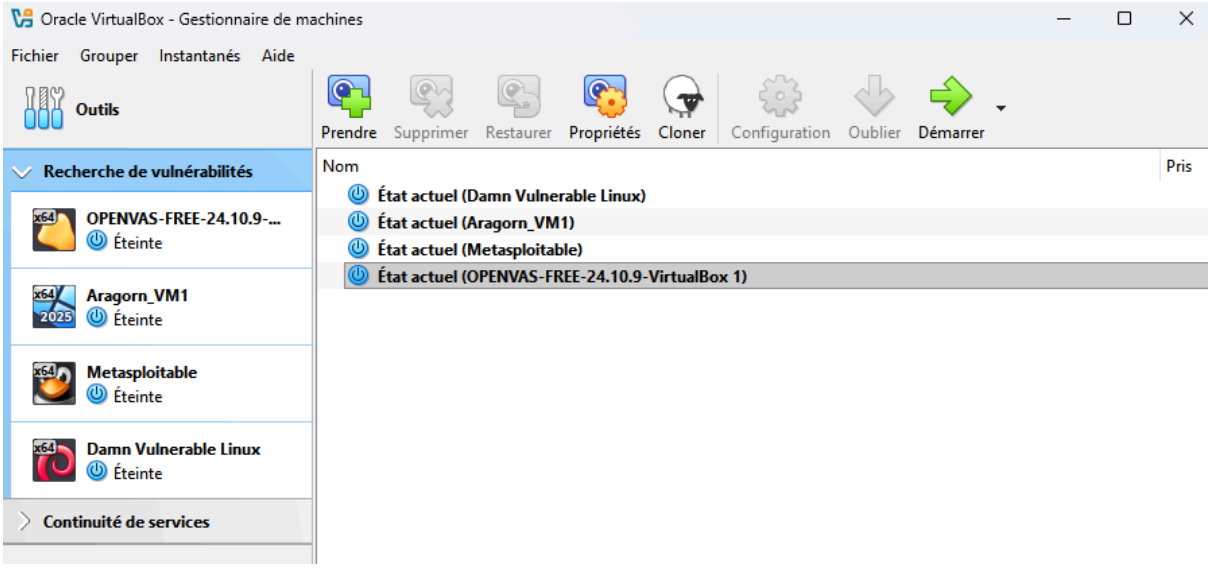
2. Installation et configuration de Damn Vulnerable Linux

Téléchargement de l'iso **debian-13.4.0-amd64-netinst.iso** sur Debian -- Téléchargement de Debian pour faire la VM Damn Vulnerable Linux

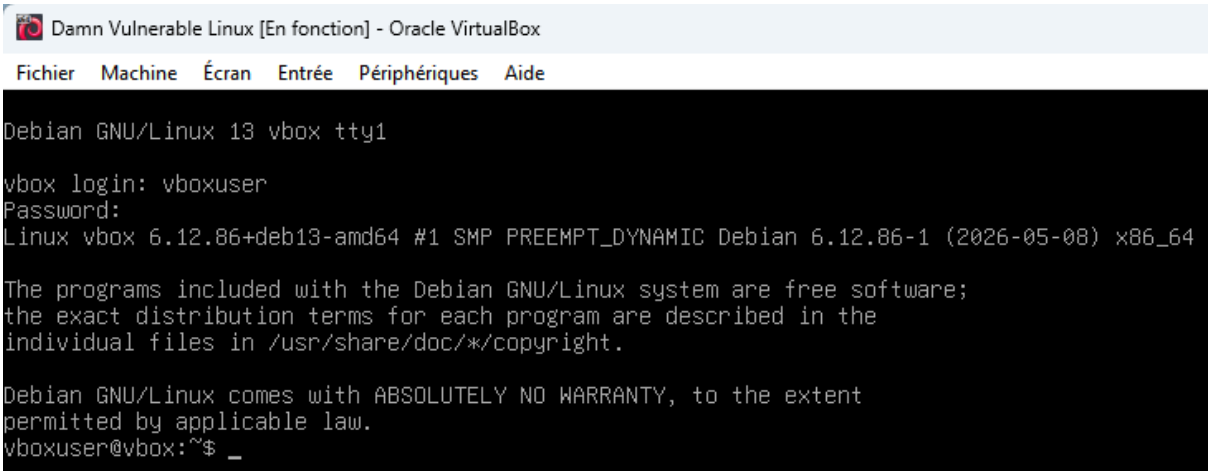


Configuration du réseau interne LABA dans VirtualBox pour isoler les machines du TP.

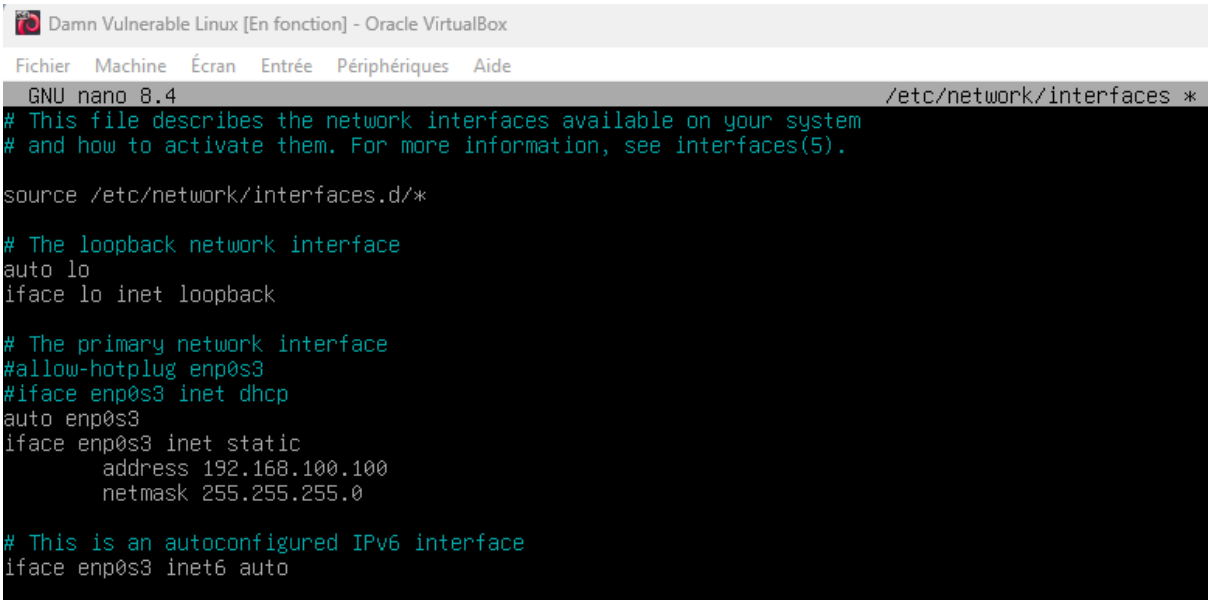




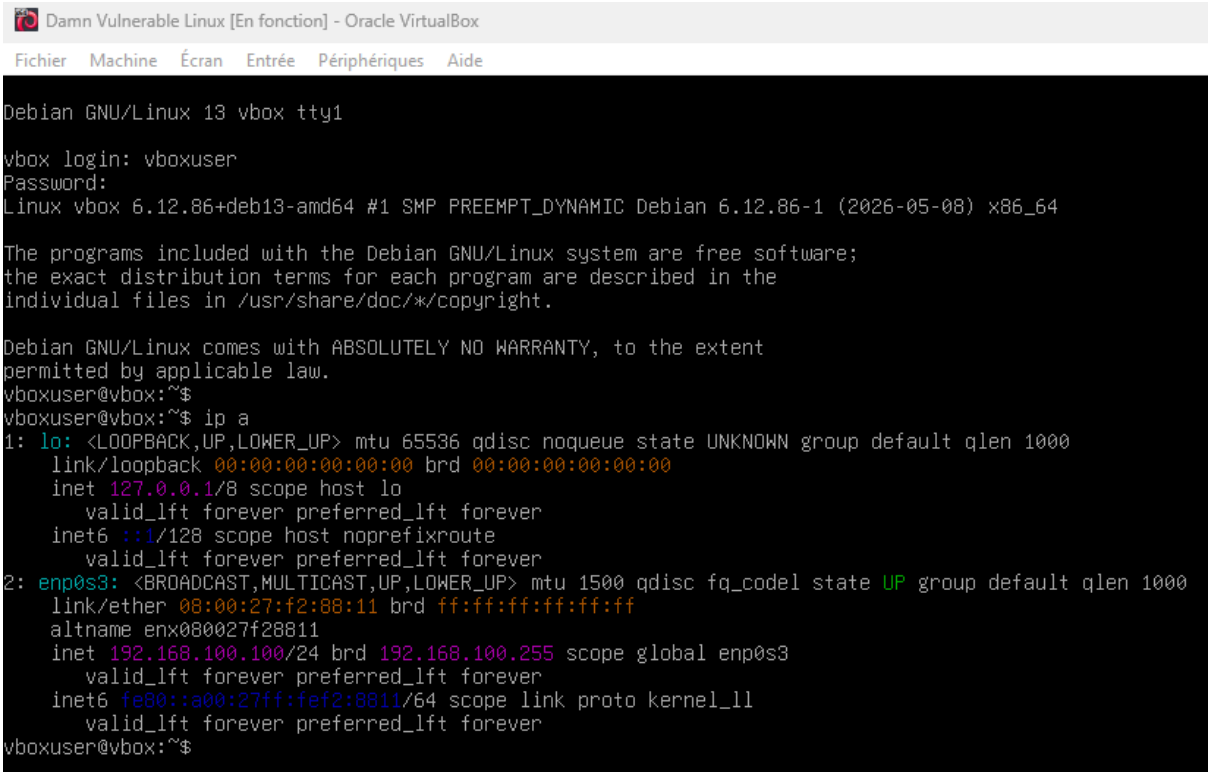
Connexion réussie à la machine virtuelle Damn Vulnerable Linux.



Modification du fichier **/etc/network/interfaces** pour configurer une adresse IP statique sur la machine Damn Vulnerable Linux.



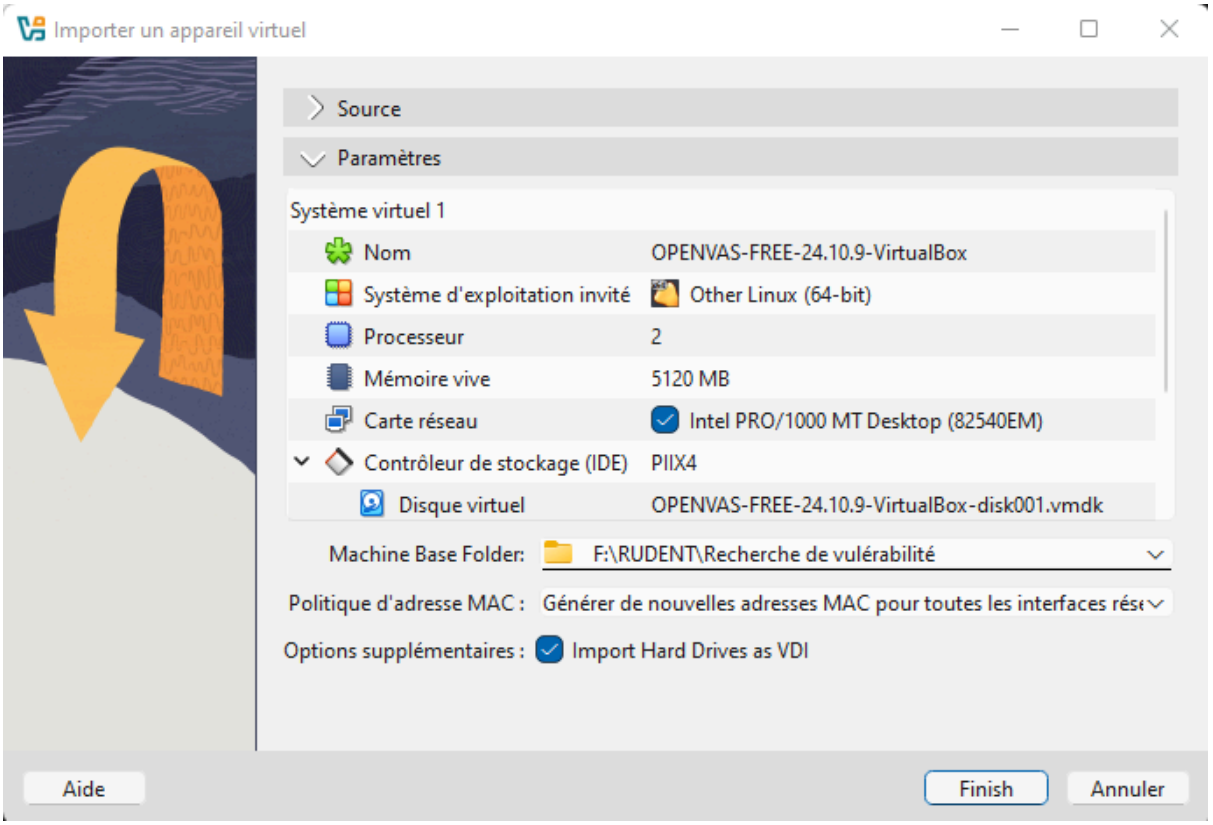
Vérification de la configuration réseau avec la commande ip a pour confirmer l'adresse IP 192.168.100.100.



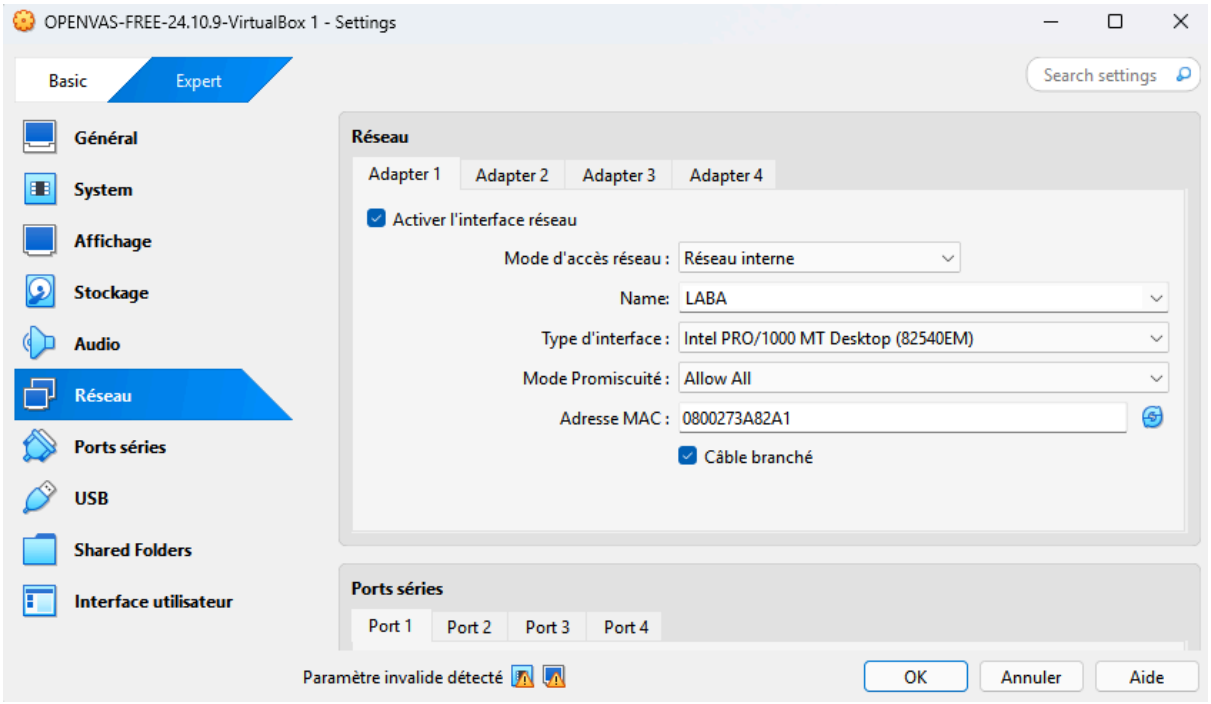
3. Installation et configuration de Greenbone

3.1 Configuration de la machine virtuelle

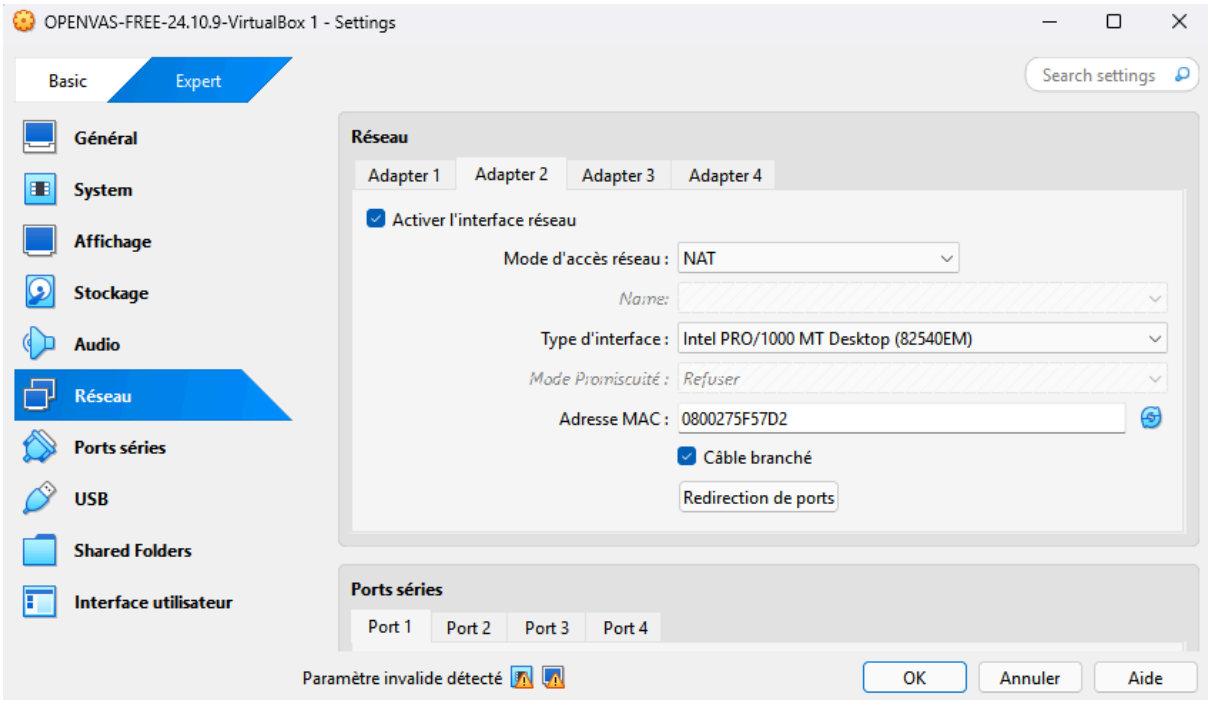
Importation de la machine virtuelle OpenVAS/Greenbone dans VirtualBox afin de préparer l'environnement de scan de vulnérabilités.



Configuration de l'interface réseau enp0s3 OpenVAS en réseau interne LABA pour communiquer avec les machines cibles.

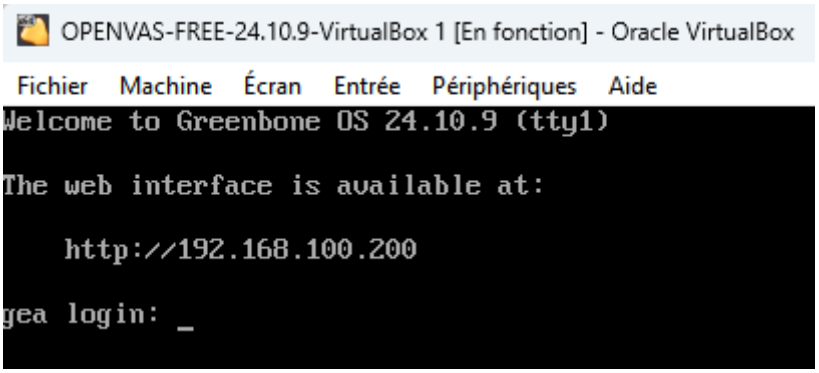


Configuration de l'interface réseau enp0s8 OpenVAS en mode NAT pour permettre l'accès à Internet et les mises à jour de Greenbone.

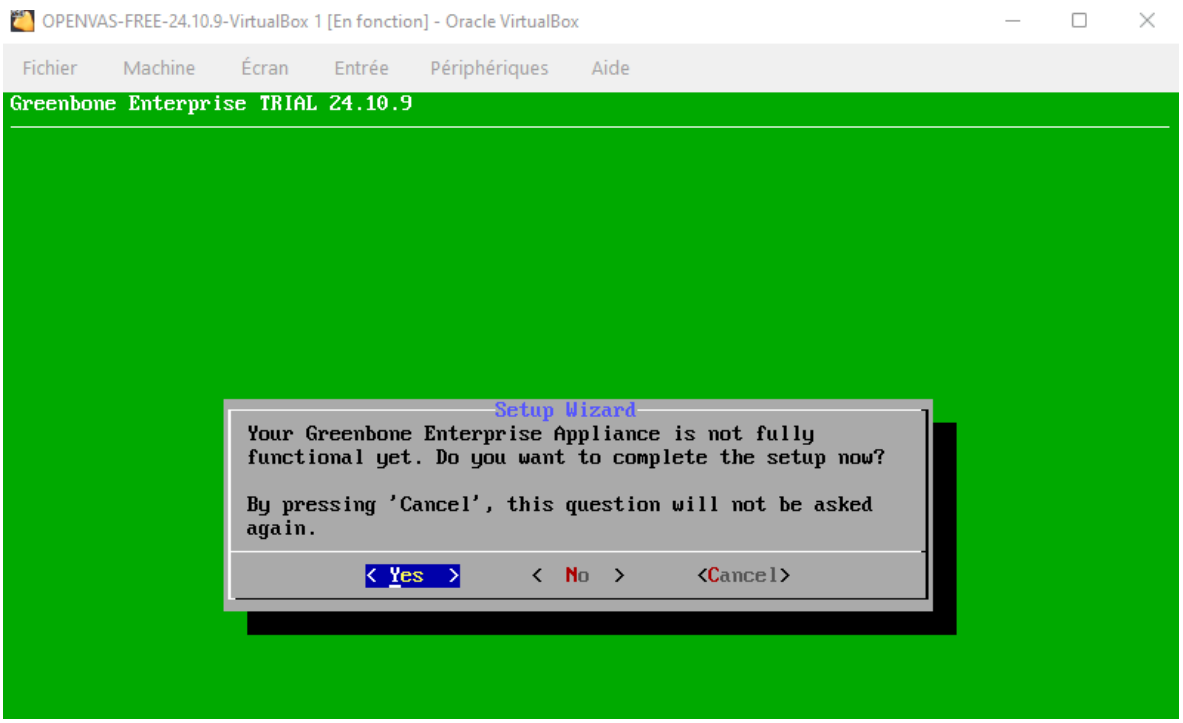


3.2 Première configuration à l'aide de l'assistant

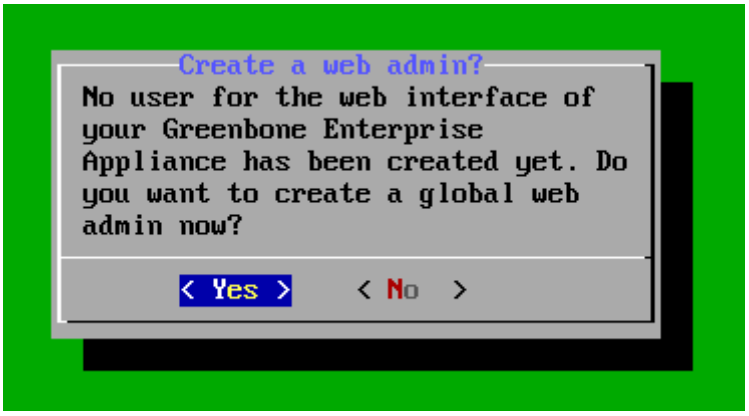
Démarrage de Greenbone et récupération de l'adresse IP permettant d'accéder à l'interface Web d'administration.



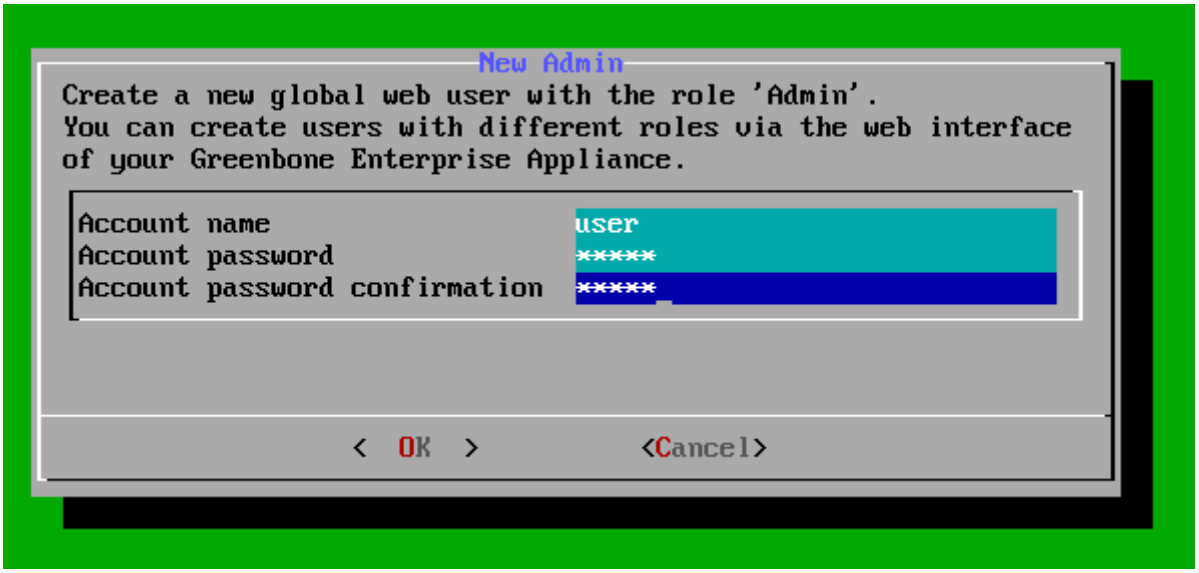
Lancement de l'assistant de configuration initiale de Greenbone afin de finaliser les paramètres du système.



Création du compte administrateur Web pour accéder à l'interface de gestion Greenbone.

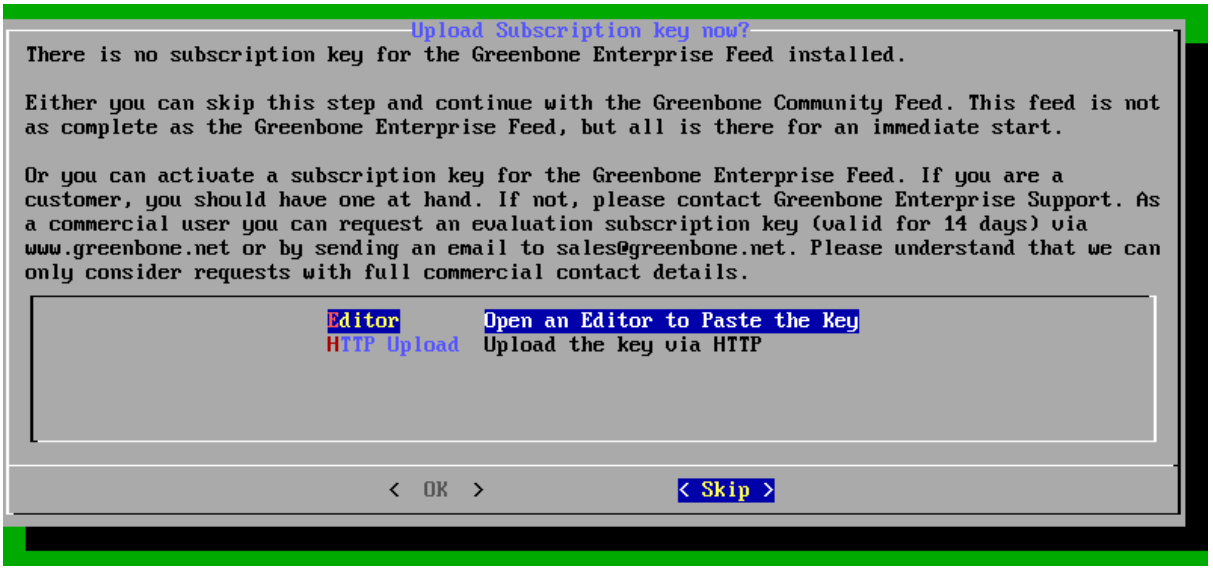


Définition du nom d'utilisateur et du mot de passe du compte administrateur Greenbone.

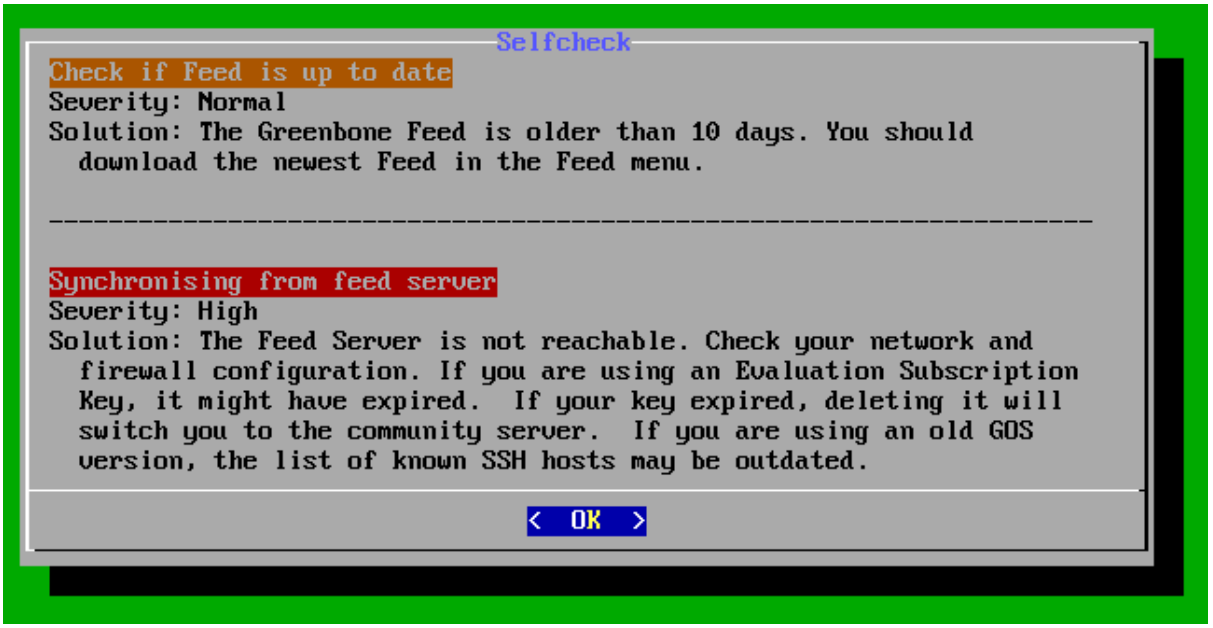


Validation de la création du compte administrateur Greenbone.

Utilisation du flux communautaire Greenbone Community Feed pour continuer la configuration sans clé de licence Enterprise.



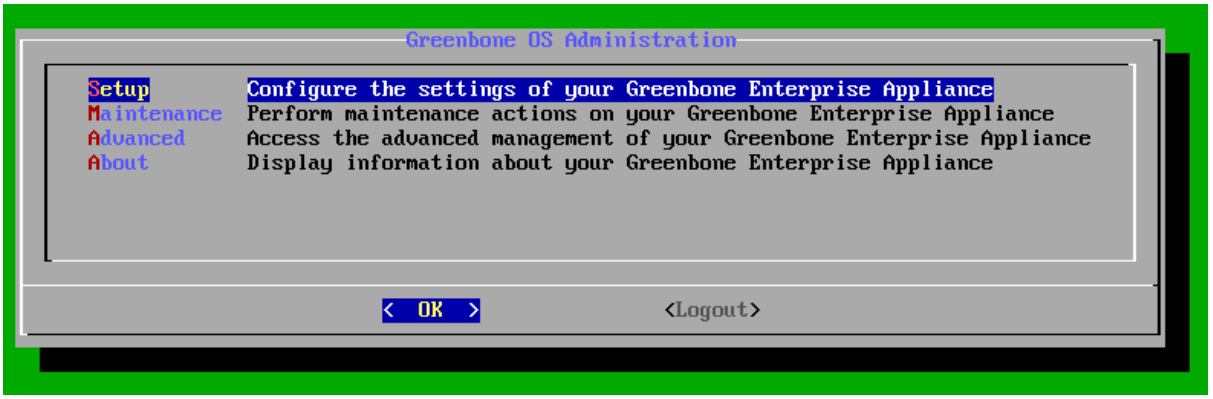
Vérification de l'état du Greenbone Feed et synchronisation des bases de vulnérabilités avec le serveur de mise à jour.



3.3 Description des menus

a) Menu général d'administration

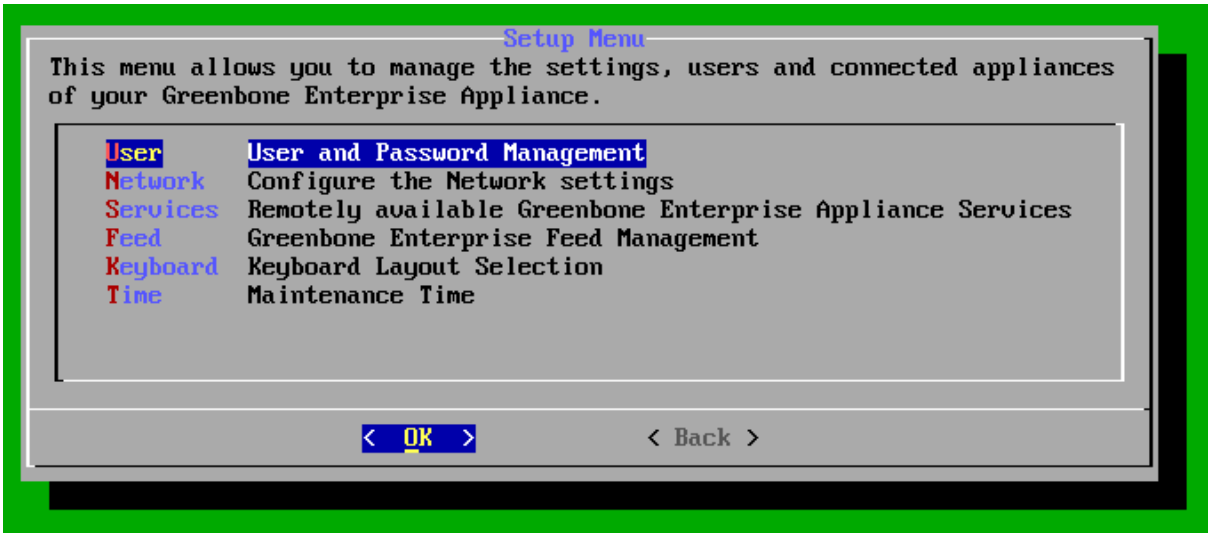
Présentation du menu d'administration principal permettant d'accéder aux fonctions de configuration, maintenance et gestion avancée de Greenbone.



- **Setup** : permet de configurer les paramètres de base du serveur (Gestion des utilisateurs, des paramètres réseau, des sources d'installation des listes de définition de vulnérabilité, configuration de la disposition du clavier...)
- **Maintenance** : permet d'effectuer la mise à jour de la liste de définition de vulnérabilité, et d'arrêter proprement la VM.
- **Advanced** : accéder à certaines fonctionnalités uniquement disponibles pour la version entreprise (nous n'utiliserons donc pas ce menu)
- **About** : Afficher des informations utiles sur le système en cours de fonctionnement (version et adresse à utiliser pour l'accès à interface Web notamment)

b) Menu Administration > Setup

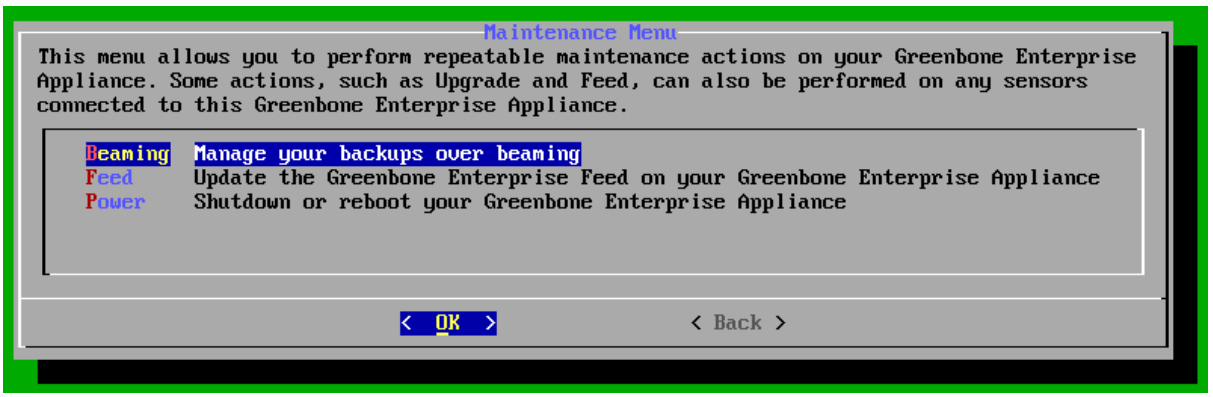
Présentation du menu Setup permettant de gérer les utilisateurs, le réseau, les services et les mises à jour de Greenbone.



- **User** : permet de gérer les utilisateurs et les privilèges (Invités, administrateur, super administrateur) ainsi que la politique de gestion des mots de passe
- **Network** : configuration des adresses IP V4 et V6 de la machine (adresse IP, Passerelle par défaut, DNS)
- **Services** : configuration des services d'administration distante au serveur Greenbone local (Serveur Web, SSH, gestion des certificats, protocoles, méthodes de chiffrement,
- **Feed** : configuration des sources de mises à jour des listes de définition des vulnérabilités.
- **Keyboard** : configuration de la disposition du clavier (NE FONCTIONNE PAS ! - Ce n'est pas bloquant, puisque l'interface Web prend en compte le clavier français)
- **Time** : Définition de l'heure des opérations de maintenance du serveur lui-même (hors mise à jour des Feeds)

c) Menu Administration > Maintenance

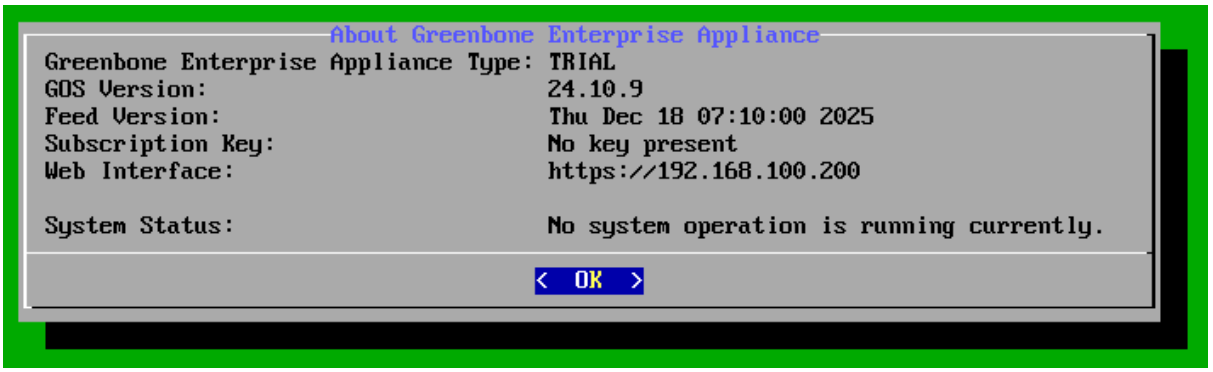
Présentation du menu Maintenance permettant d'effectuer les sauvegardes, les mises à jour et le redémarrage du système Greenbone.



- **Beaming** : permet de répliquer la configuration d'un serveur Greenbone sur un autre serveur Greenbone (utilisable uniquement dans la version entreprise)
- **Feed** : lance une opération de mise à jour des listes de définition des vulnérabilités
- **Power** : permet d'arrêter le serveur

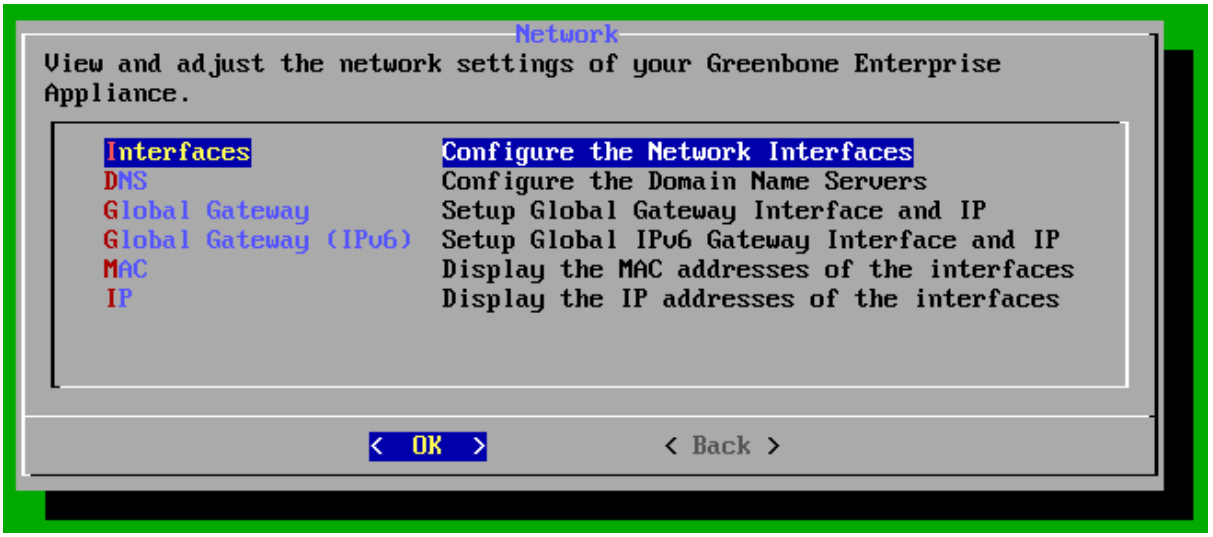
d) Menu Administration > About

Présentation du menu About affichant les informations système, la version de Greenbone et l'adresse de l'interface Web.

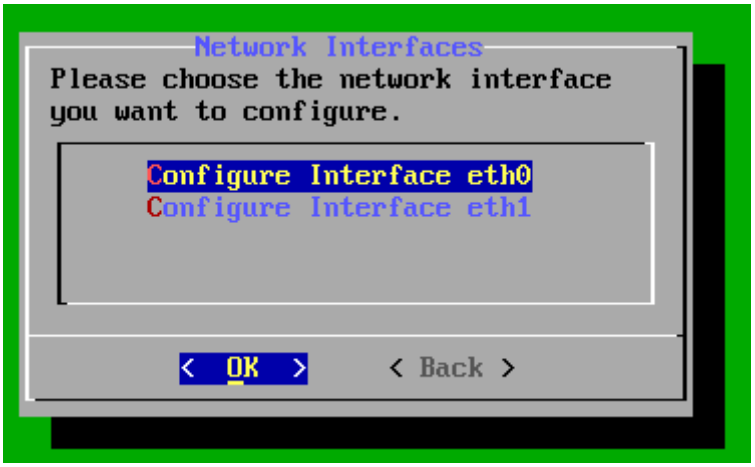


3.4 Configuration du réseau

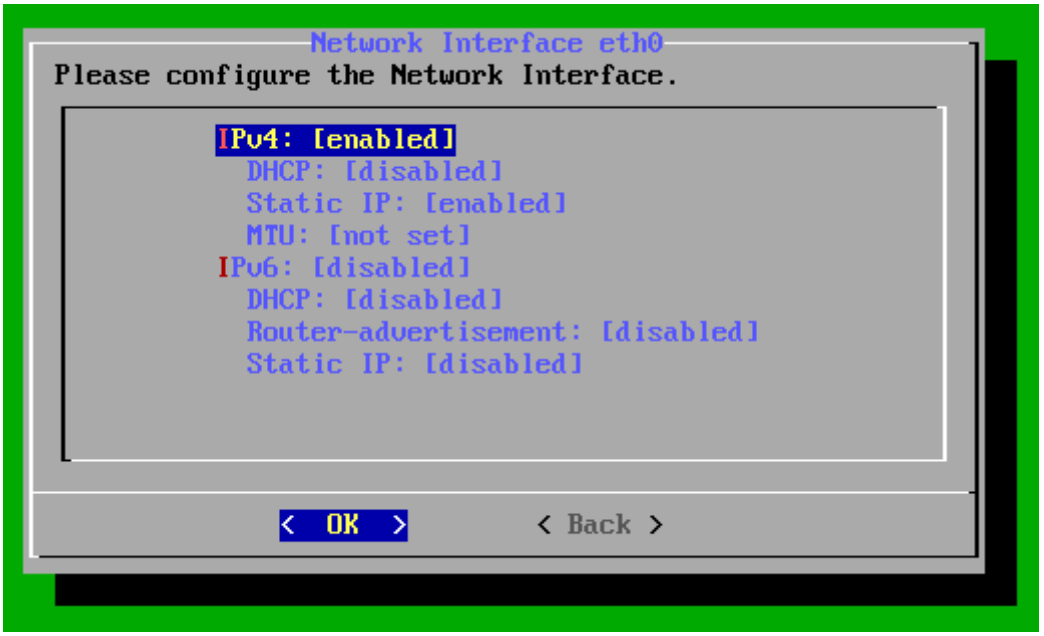
Accès au menu réseau de Greenbone pour configurer les interfaces réseau, les adresses IP et les serveurs DNS.



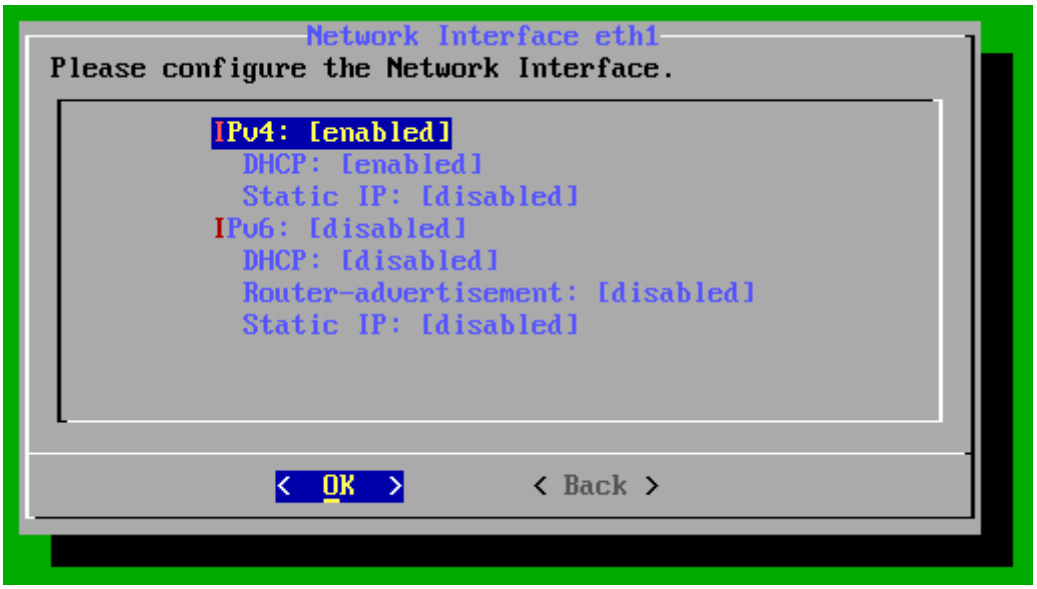
Sélection de l'interface réseau à configurer sur la machine Greenbone.



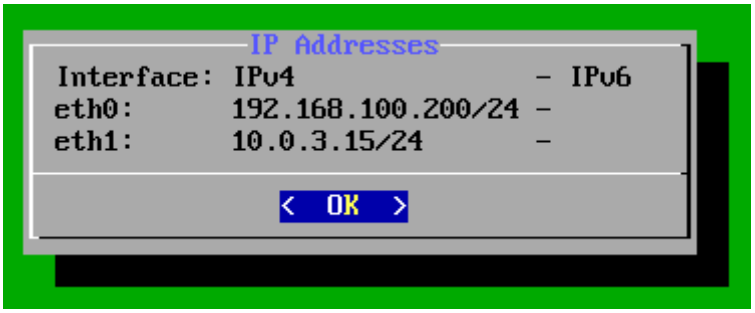
Configuration de l'interface réseau **eth0** avec une adresse IPv4 statique pour le réseau interne du laboratoire.



Configuration de l'interface réseau **eth1** en DHCP pour permettre l'accès Internet et les mises à jour Greenbone.

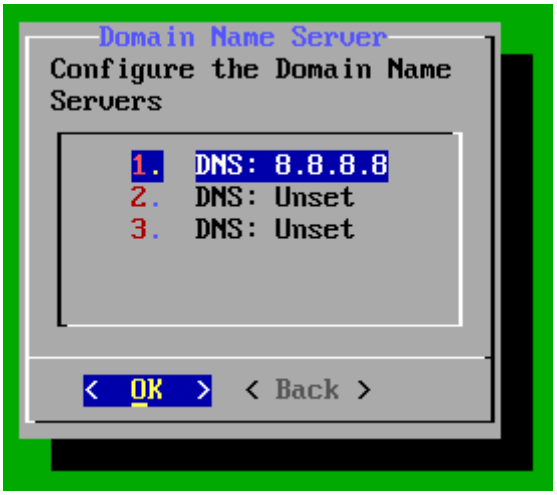


Vérification des adresses IP configurées sur les interfaces réseau de Greenbone.

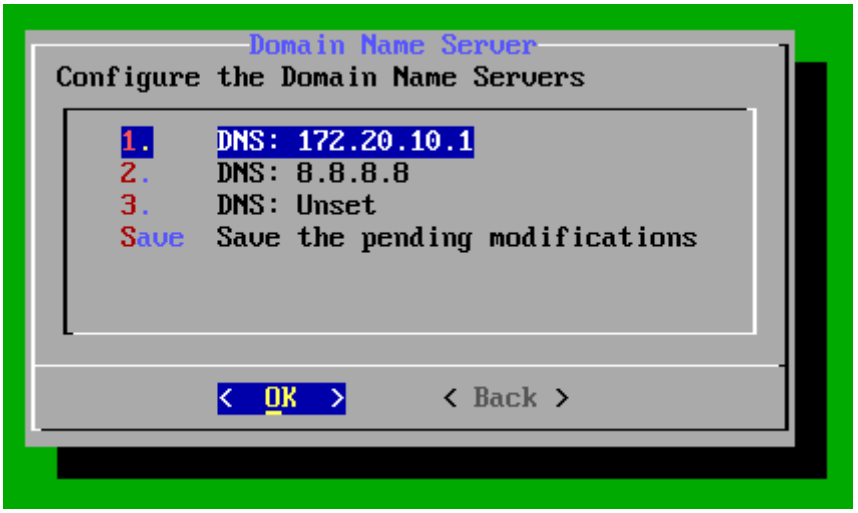


Validation et sauvegarde de la nouvelle configuration réseau du système.

Configuration du serveur DNS Google 8.8.8.8 pour permettre la résolution de noms et les mises à jour Internet.



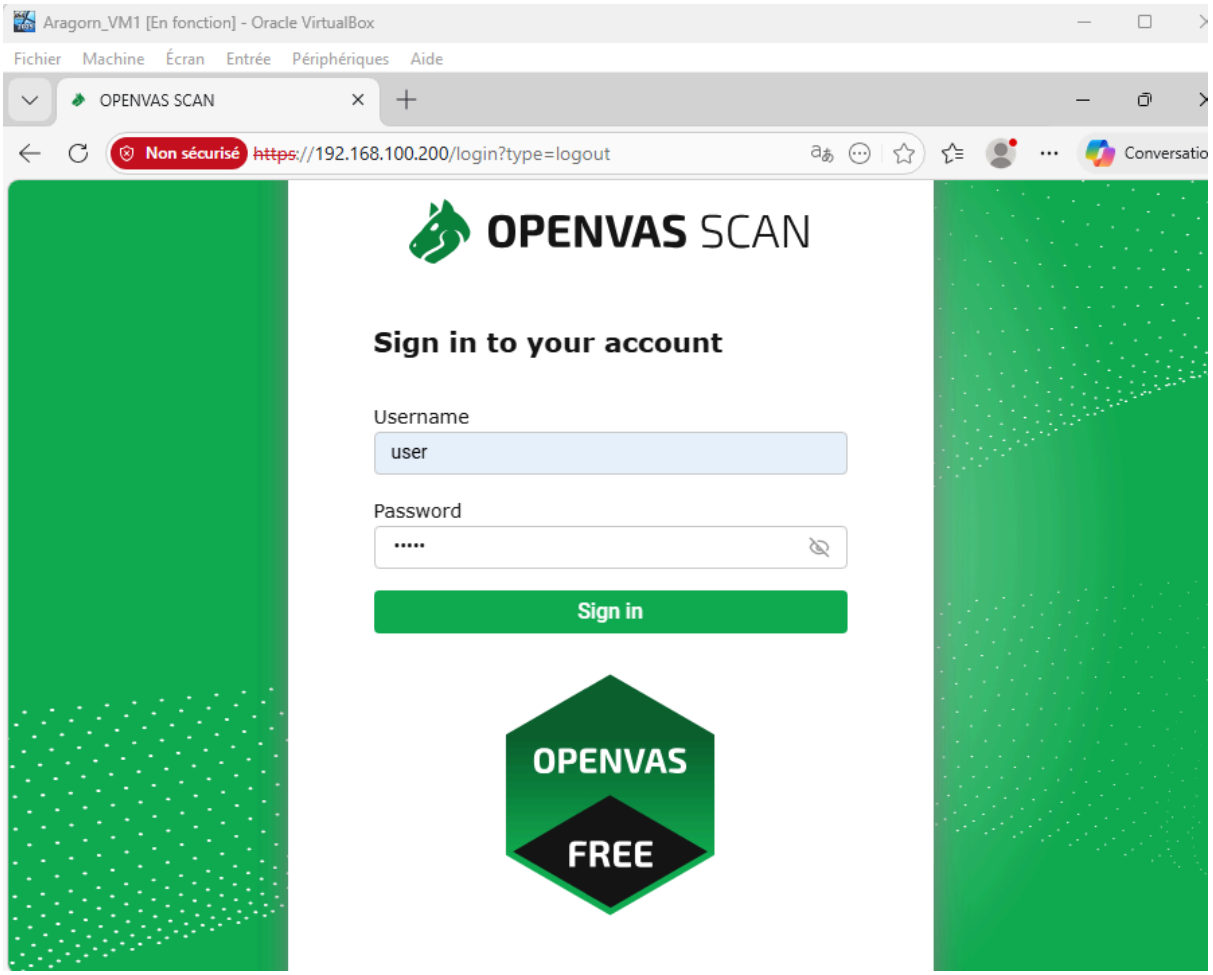
Ajout des serveurs DNS pour permettre l'accès réseau et les mises à jour de Greenbone.



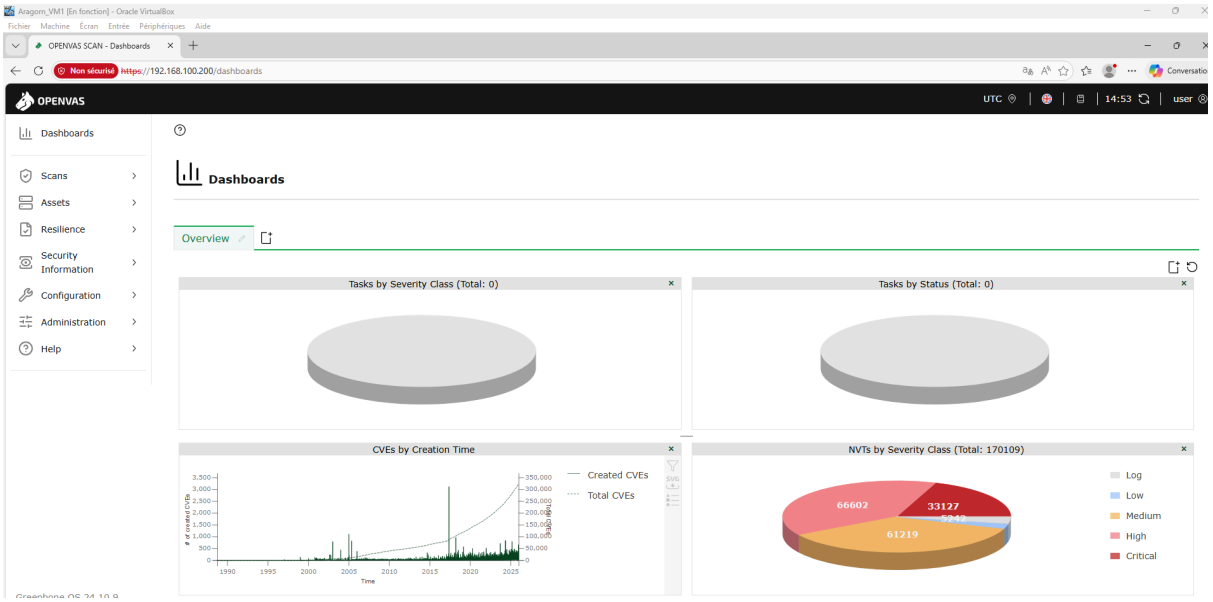
Validation et enregistrement des paramètres DNS configurés sur le système.

3.5 Connexion interface Web

Connexion à l'interface Web OpenVAS/Greenbone depuis un navigateur afin d'accéder aux fonctions de scan de vulnérabilités.

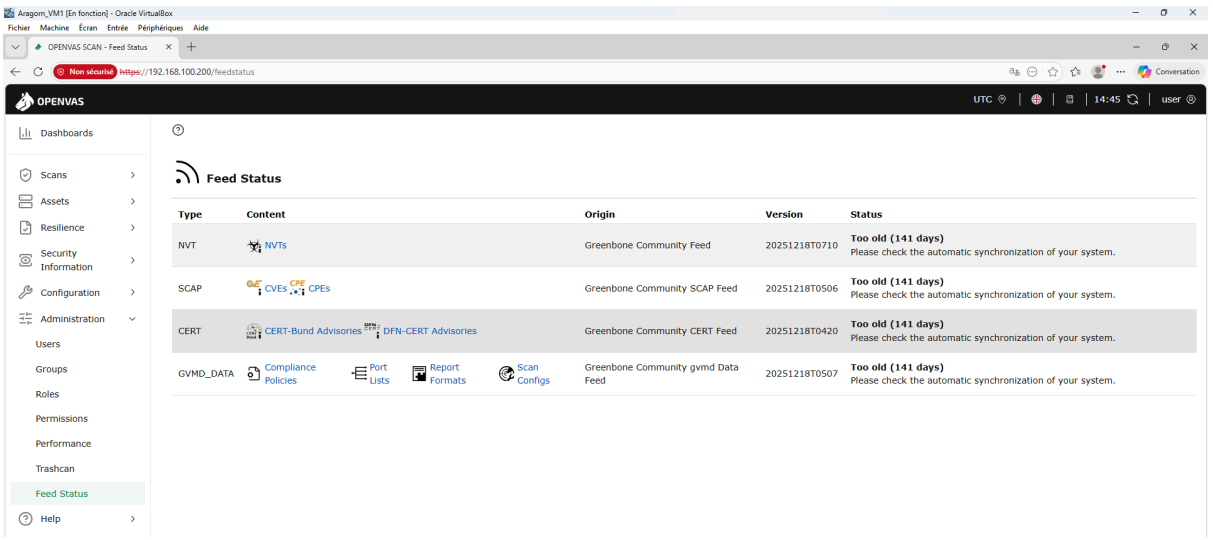


Accès au tableau de bord OpenVAS permettant de visualiser les scans, les vulnérabilités et les statistiques de sécurité.



3.6 Mise à jour des listes de définition de vulnérabilité

Vérification de l'état et de la synchronisation des bases de vulnérabilités Greenbone Community Feed.



- **NVT (network vulnerability test)** : ce sont des scripts qui sont exécutés sur un systèmes ciblés afin de vérifier la présence de failles. Certains scripts sont génériques et exécutés sur l'ensemble des actifs du réseau, tandis que d'autres ciblent particulièrement un matériel, un logiciel, un service, une version particulière d'un protocole…

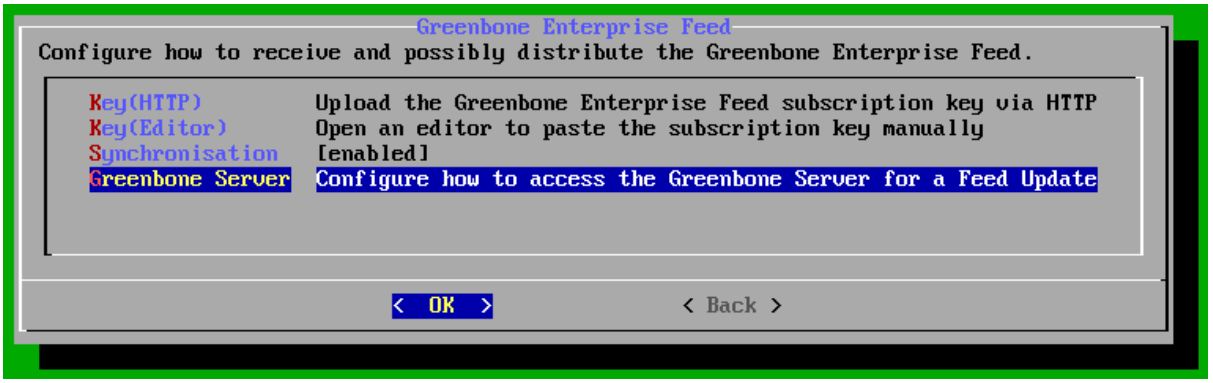
- **CVE (common vulnerabilities and exposures)** : c'est un dictionnaire de vulnérabilités de sécurité, maintenu par l'organisme MITRE et soutenu par le Département de la sécurité intérieure des USA. Les informations y sont standardisées et rendues publiques.

- **CERT (computer emergency response team)** : c'est un autre dictionnaire de vulnérabilité de sécurité, maintenu par les différents CERT et CSIRT (computer security incident response team) au niveau mondial.

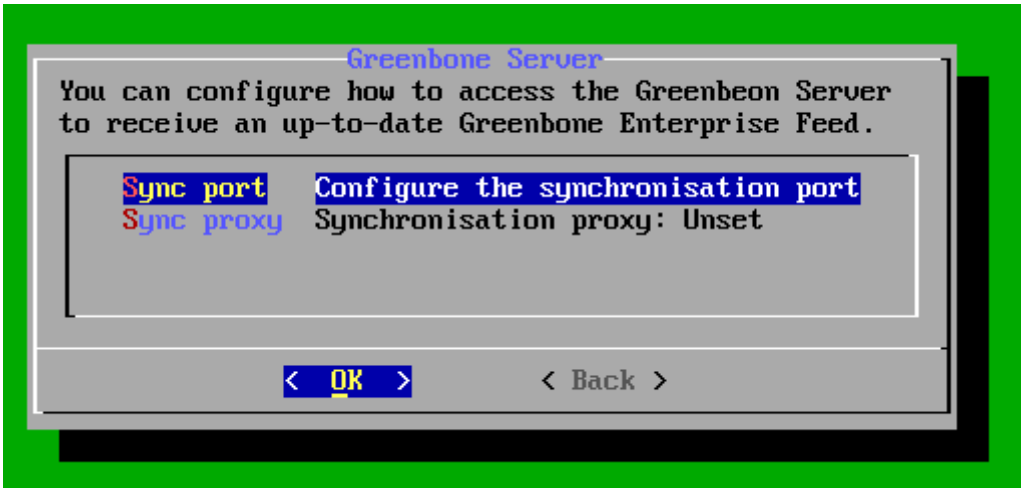
- **GVDM_DATA** : contient les paramètres utilisés par défaut par Greenbone lors de la recherche de vulnérabilité, de la classification des risques et de la génération de rapports.

e) Configuration du serveur de mise à jour

Accès au menu de configuration du serveur de mise à jour Greenbone Enterprise Feed.



Configuration du port de synchronisation utilisé pour télécharger les mises à jour des bases de vulnérabilités.

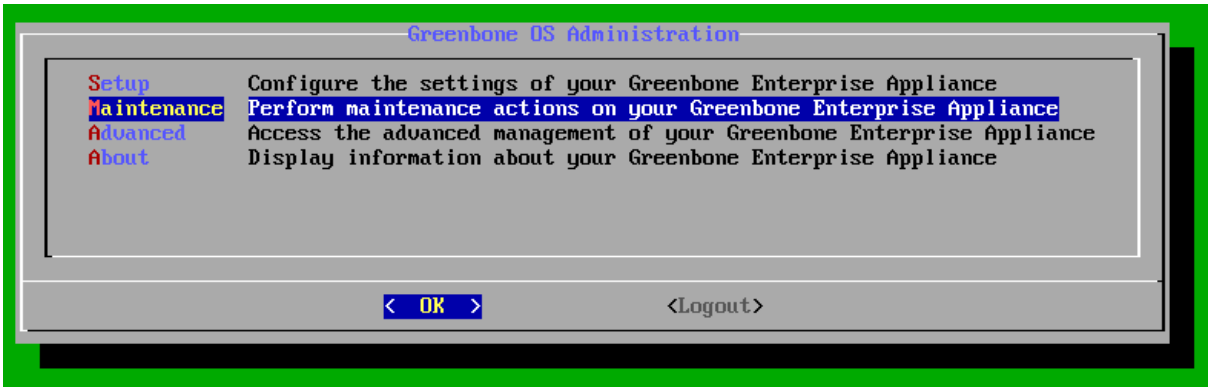


Sélection du port HTTPS 443 pour sécuriser la synchronisation des mises à jour Greenbone.

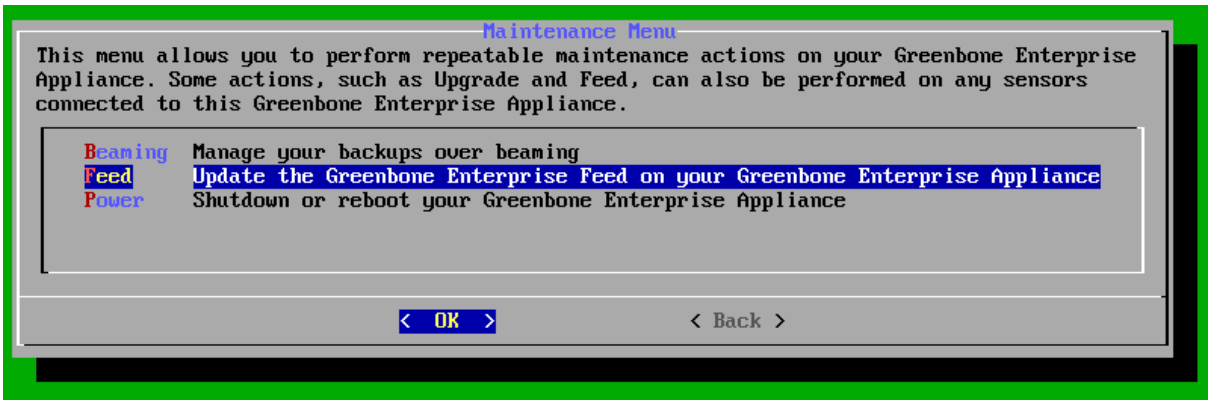
Validation de la nouvelle configuration du port de synchronisation du serveur de mise à jour.

f) Mise à jour

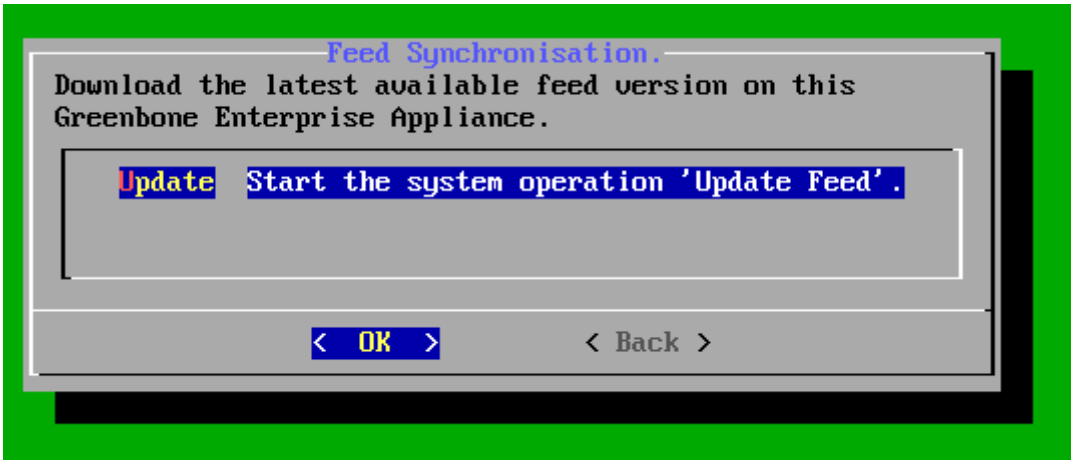
Accès au menu Maintenance afin d'effectuer les opérations de mise à jour et de maintenance de Greenbone.



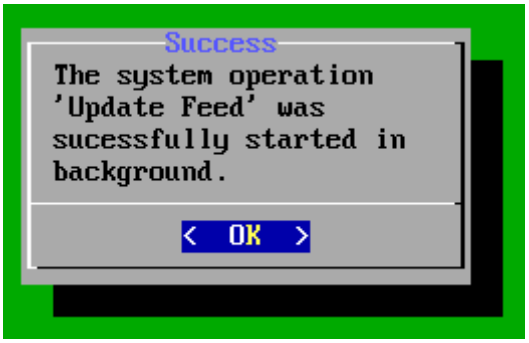
Sélection du menu Feed dans Maintenance pour lancer la mise à jour des bases de vulnérabilités Greenbone.



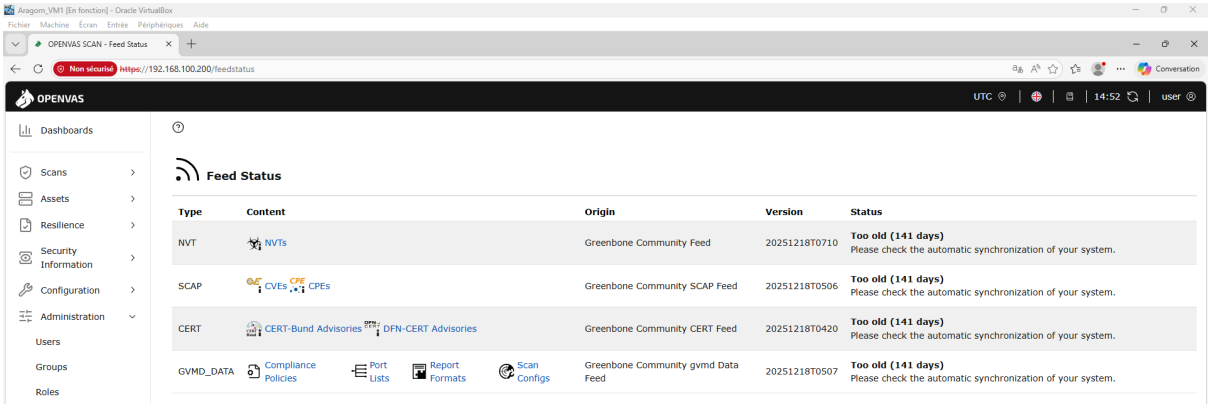
Démarrage de l'opération de synchronisation "Update Feed" afin de télécharger les dernières signatures de vulnérabilités.



Confirmation du lancement de la mise à jour des bases de vulnérabilités Greenbone en arrière-plan.

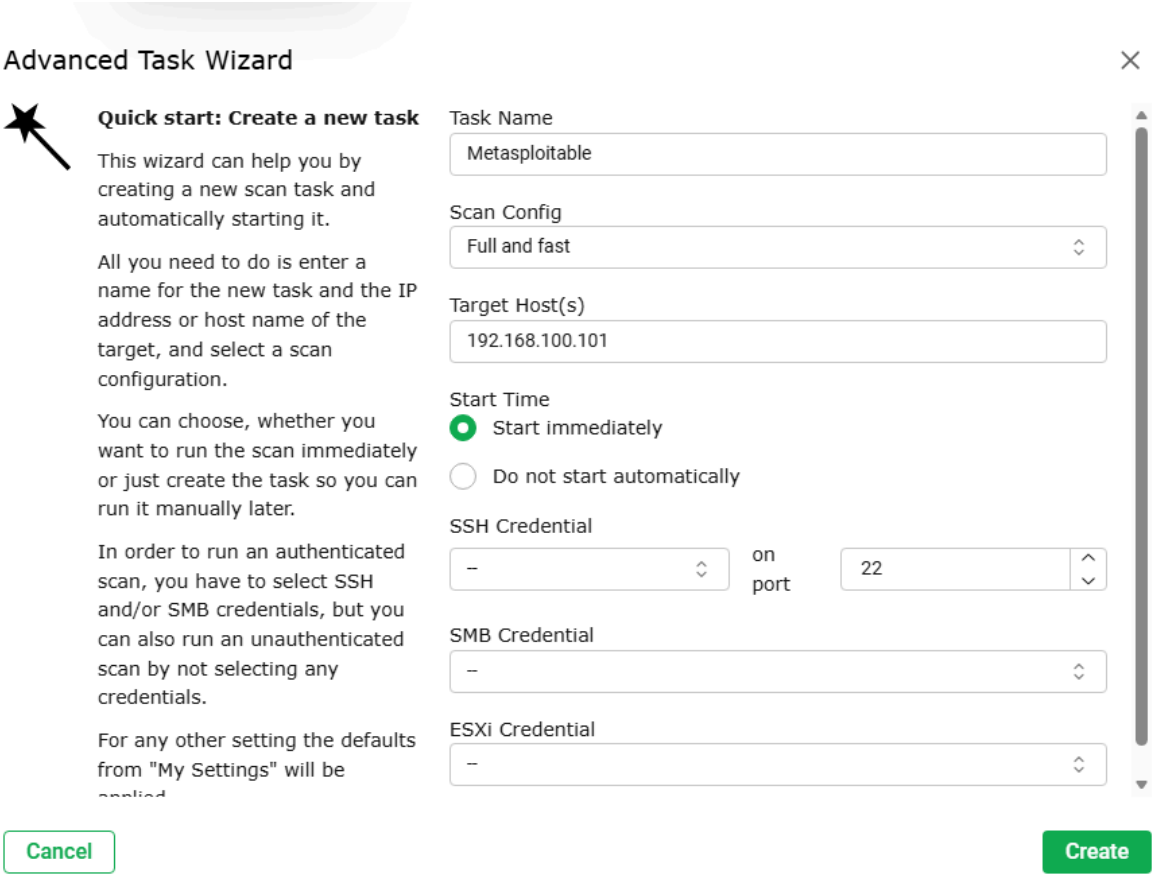


Vérification de l'état des différents flux de mise à jour depuis l'interface Web OpenVAS.

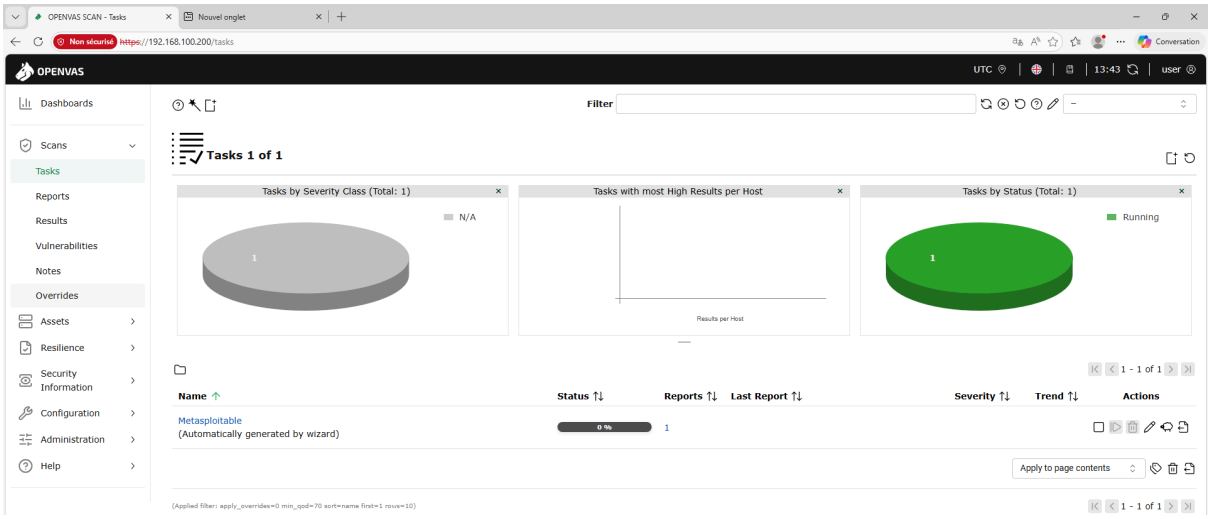


4. Test avec la VM Metasploitable

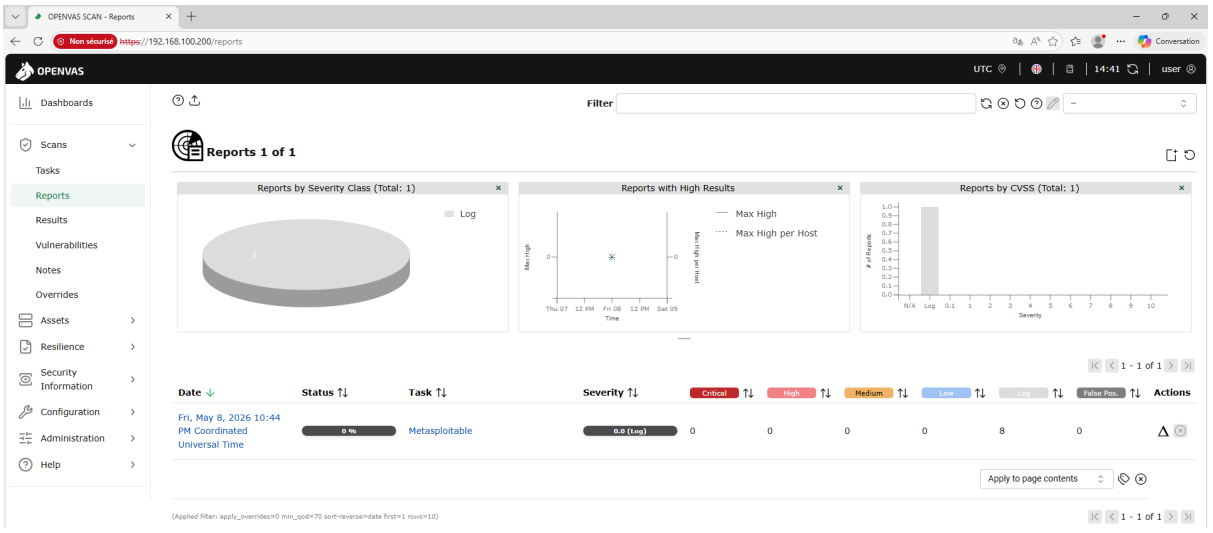
Création d'une tâche de scan OpenVAS pour analyser la machine vulnérable Metasploitable avec le profil "Full and fast".



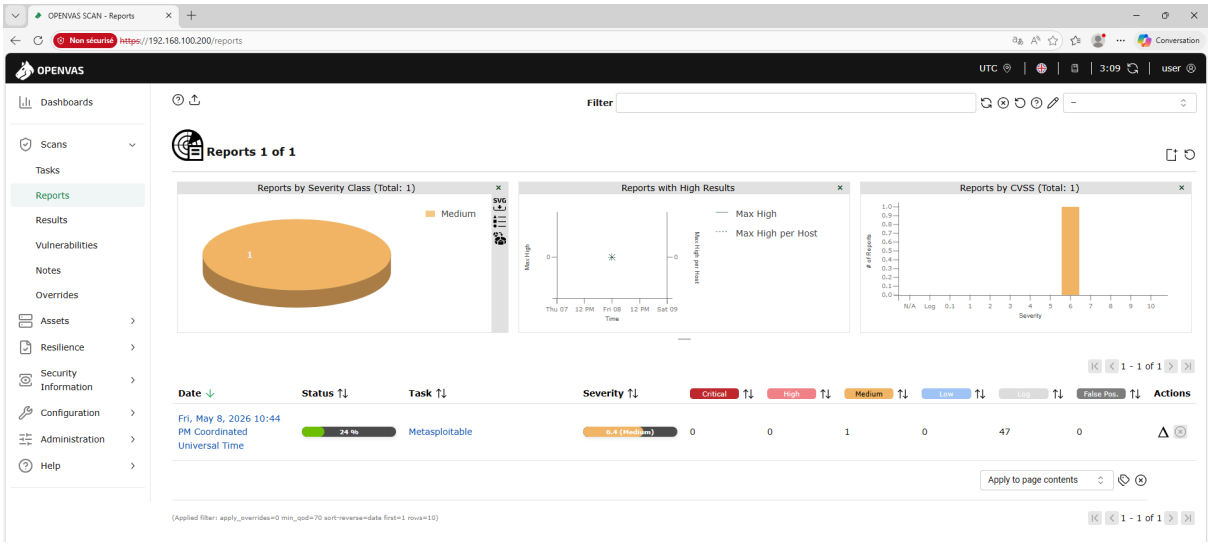
Lancement du scan de vulnérabilités sur la machine Metasploitable depuis OpenVAS.



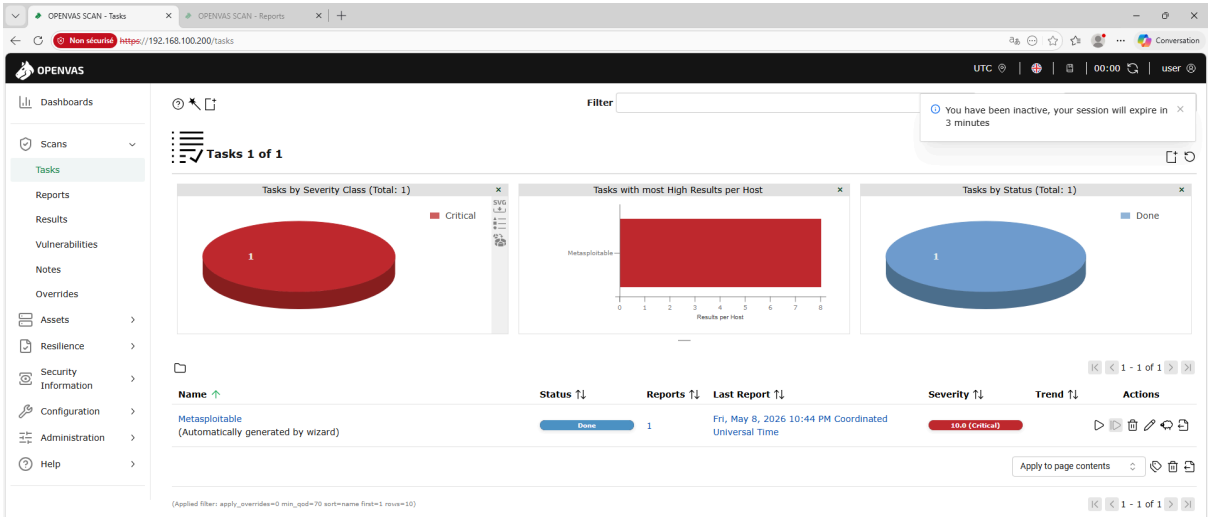
Consultation du rapport généré après l'analyse de la machine Metasploitable.



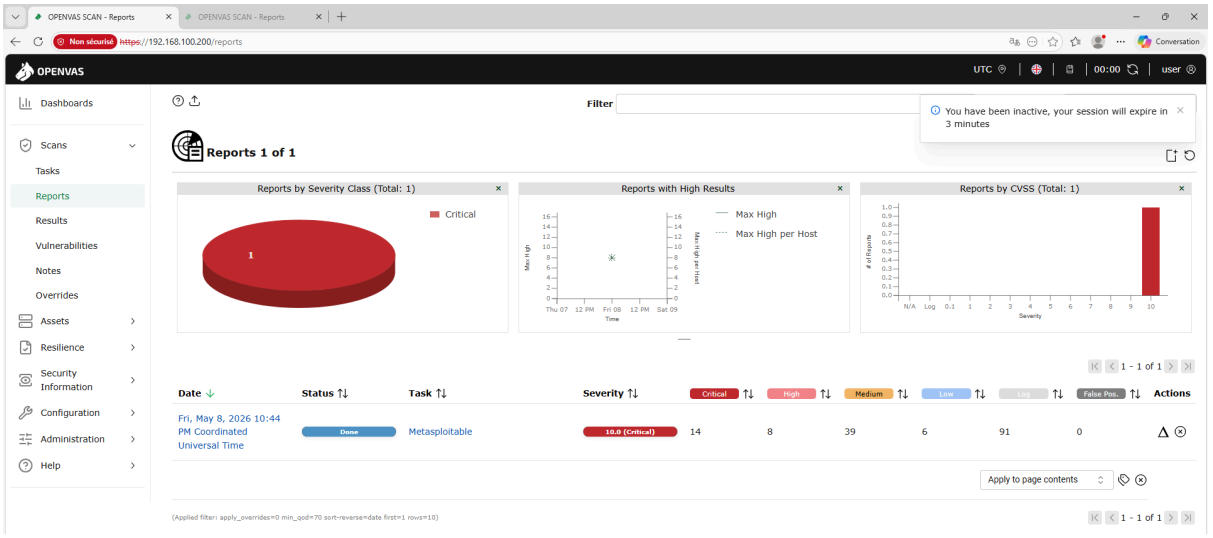
Analyse des résultats du scan Metasploitable montrant les vulnérabilités détectées et leur niveau de sévérité.



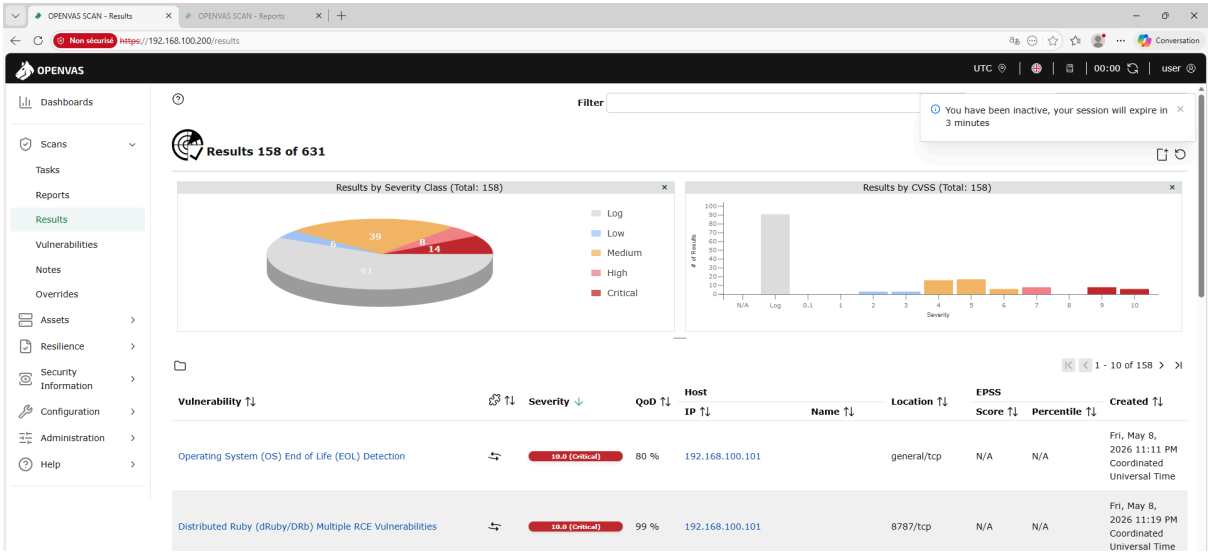
Consultation du tableau de bord des tâches OpenVAS après la fin du scan de sécurité.



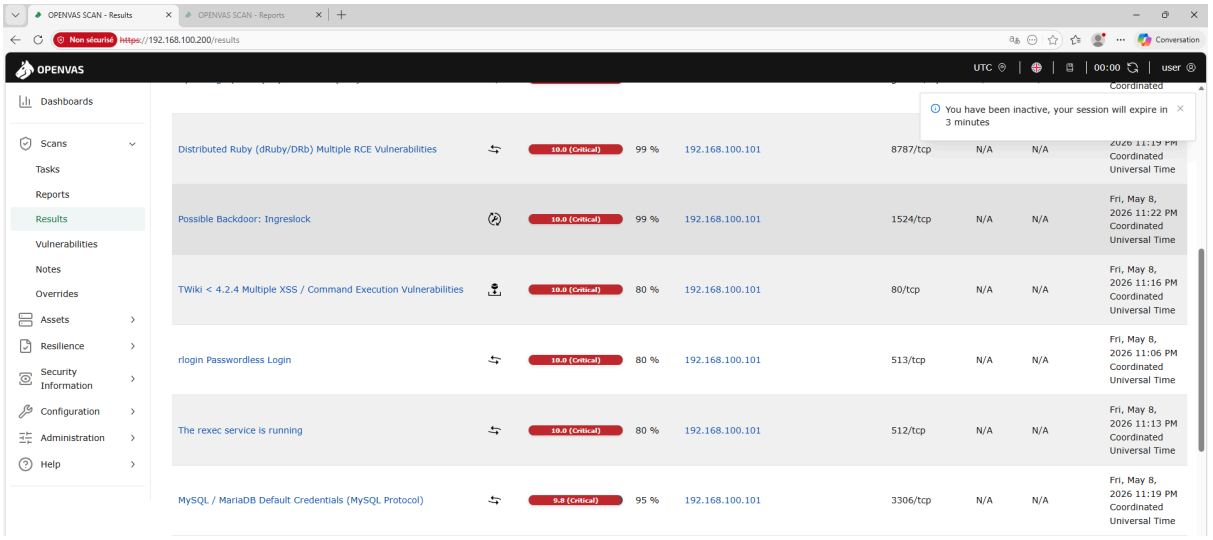
Affichage du rapport final du scan Metasploitable avec un score de sévérité critique détecté par OpenVAS.



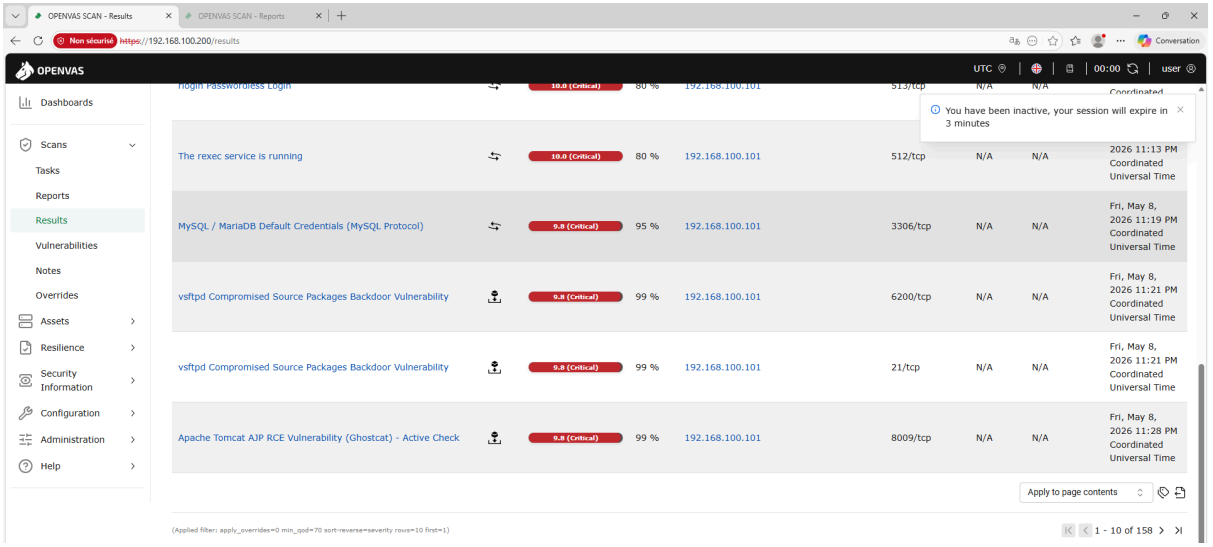
Consultation détaillée des vulnérabilités détectées, des ports ouverts et des scores CVSS associés.



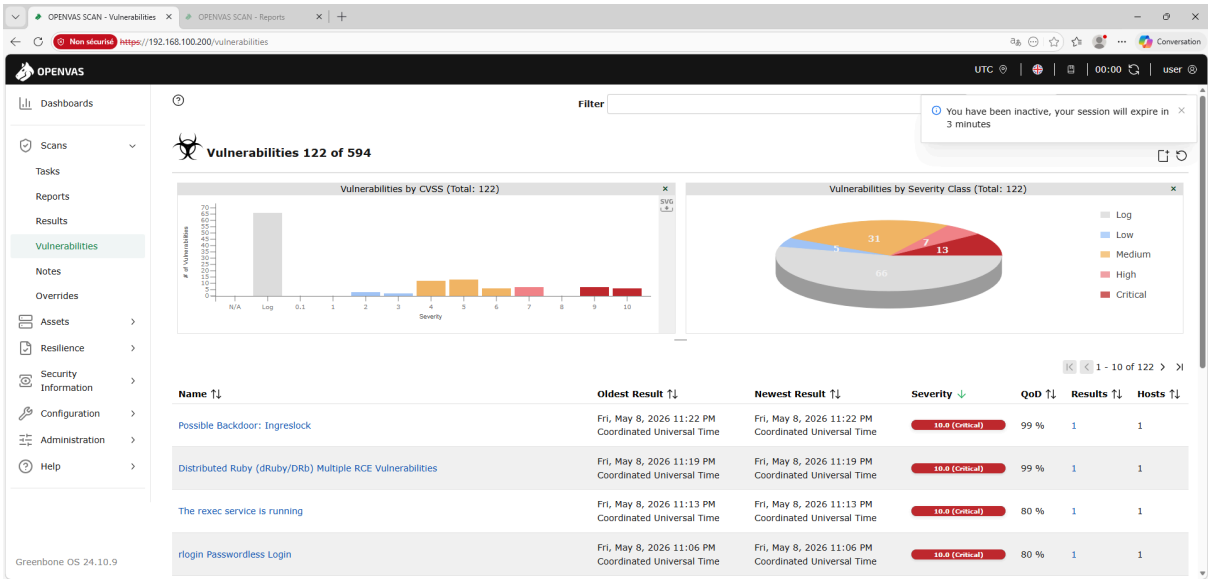
Affichage des vulnérabilités critiques détectées sur la machine Metasploitable après l'analyse OpenVAS.



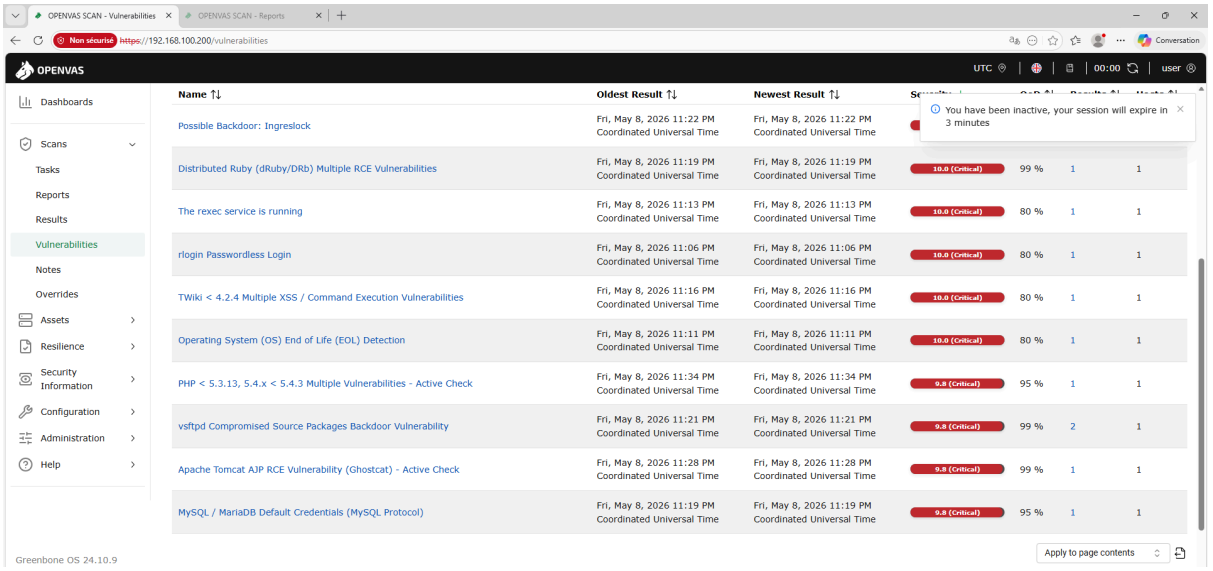
Consultation détaillée des failles de sécurité identifiées avec leurs niveaux de criticité et services associés.



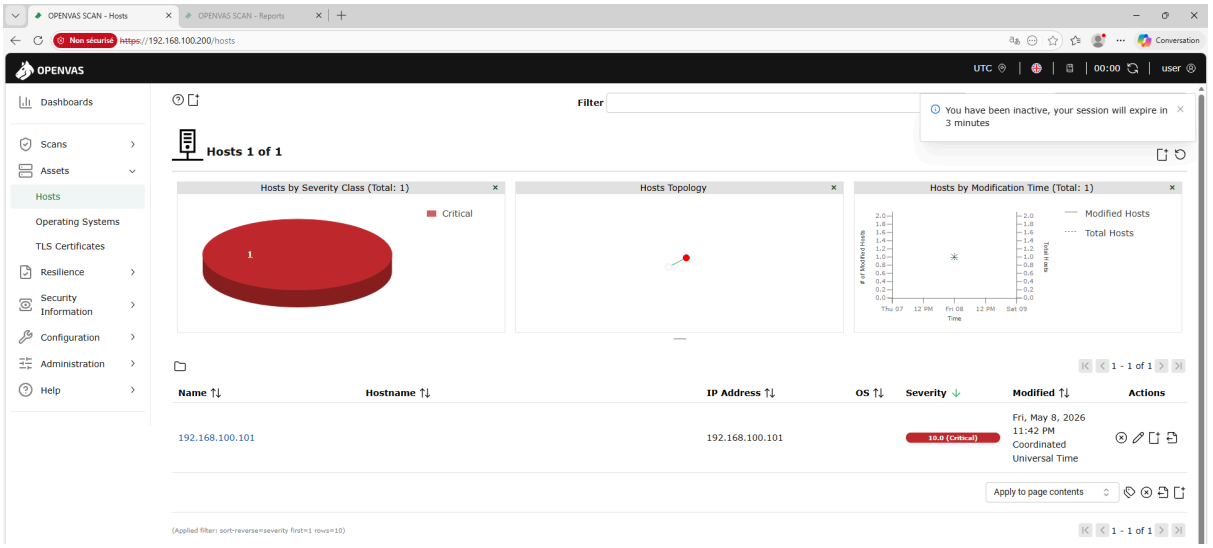
Affichage de la liste des vulnérabilités détectées par OpenVAS avec leur niveau de sévérité.



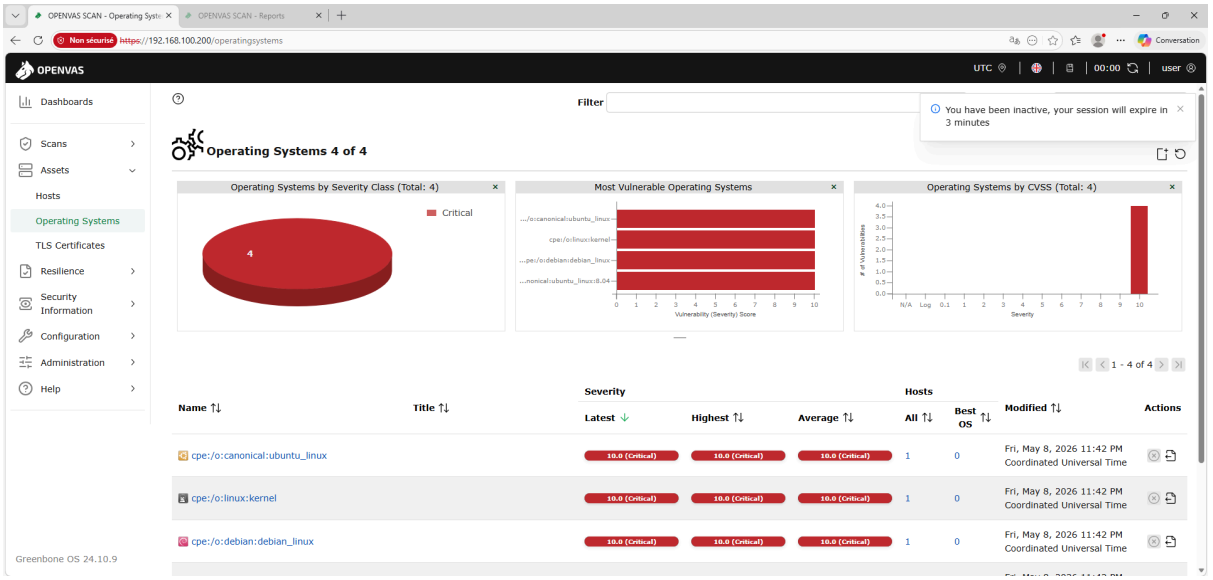
Analyse détaillée des failles de sécurité critiques présentes sur la machine Metasploitable.



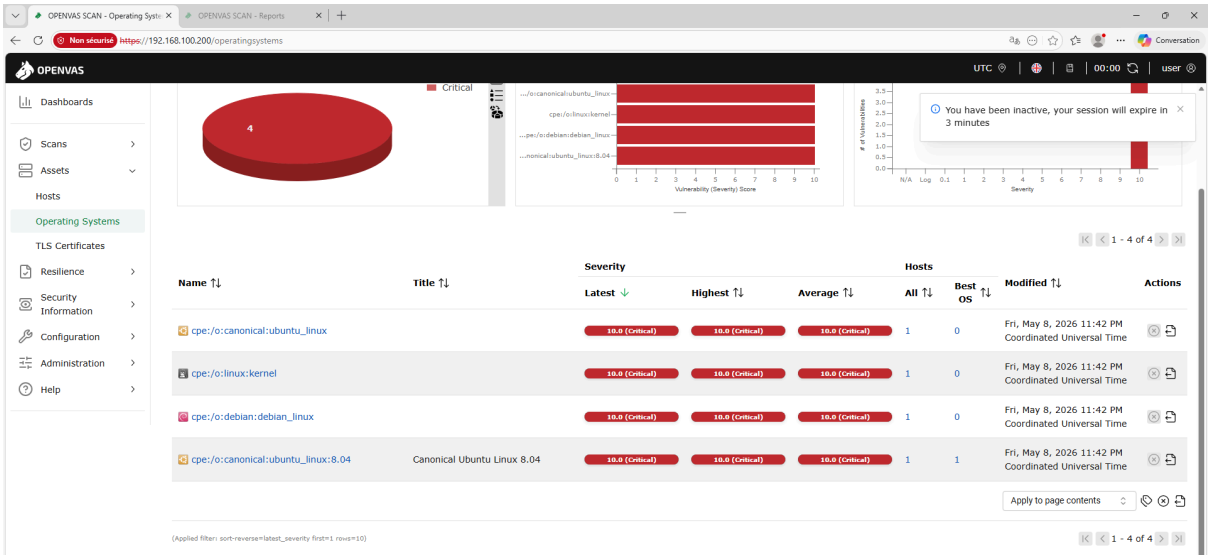
Consultation des informations sur l'hôte analysé, notamment l'adresse IP et le niveau de sévérité détecté.



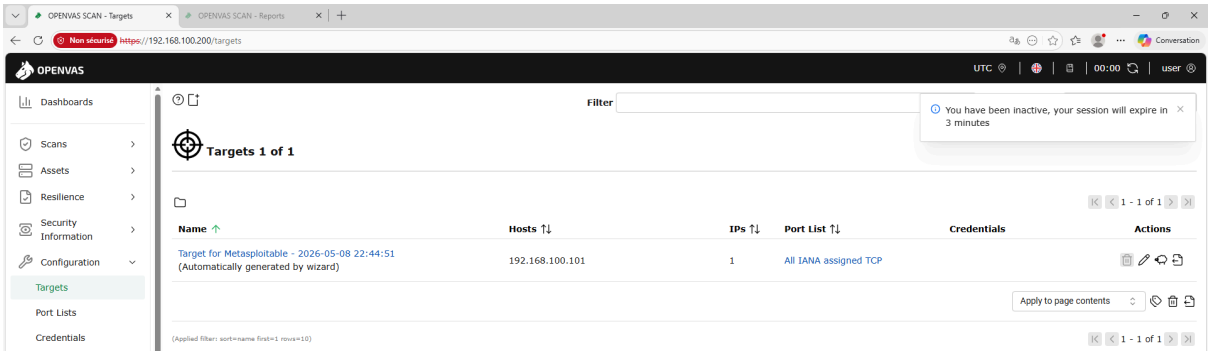
Identification des systèmes d'exploitation détectés par OpenVAS lors du scan de vulnérabilités.



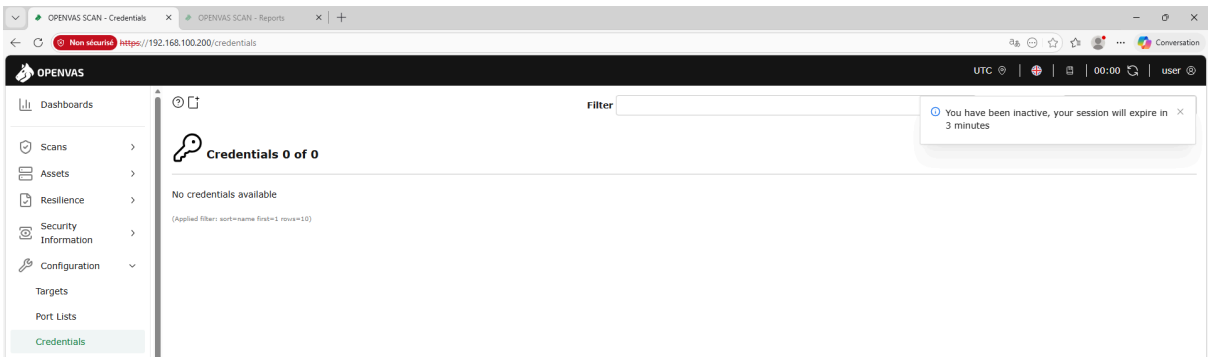
Affichage des systèmes d'exploitation détectés et de leur niveau de criticité associé.



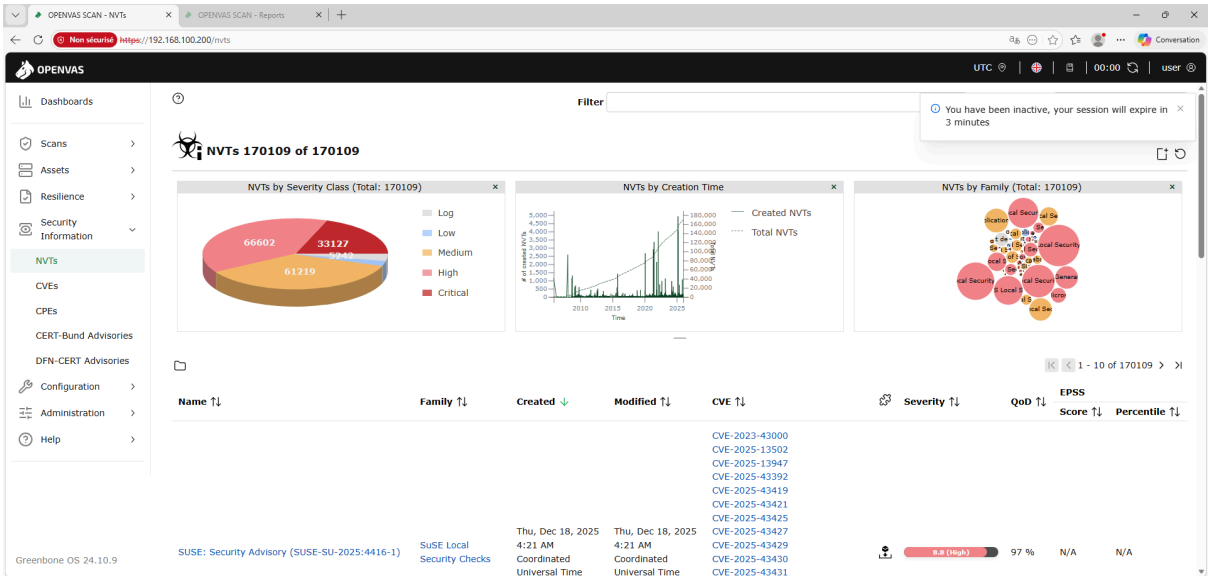
Consultation de la cible configurée dans OpenVAS pour le scan de la machine Metasploitable.



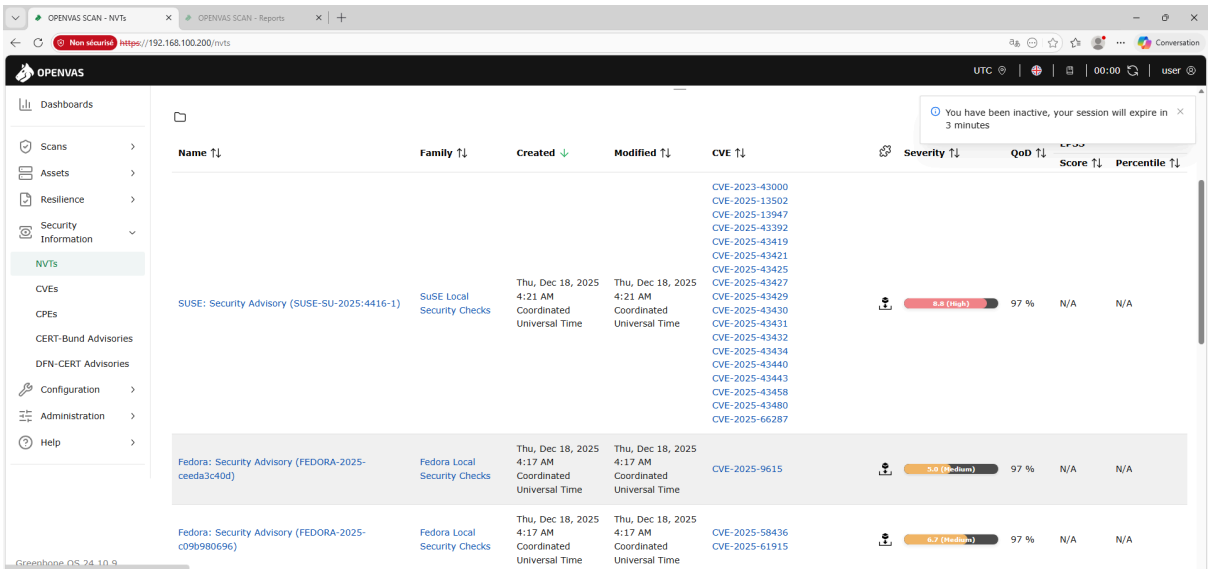
Vérification de l'absence d'identifiants configurés pour les scans authentifiés.



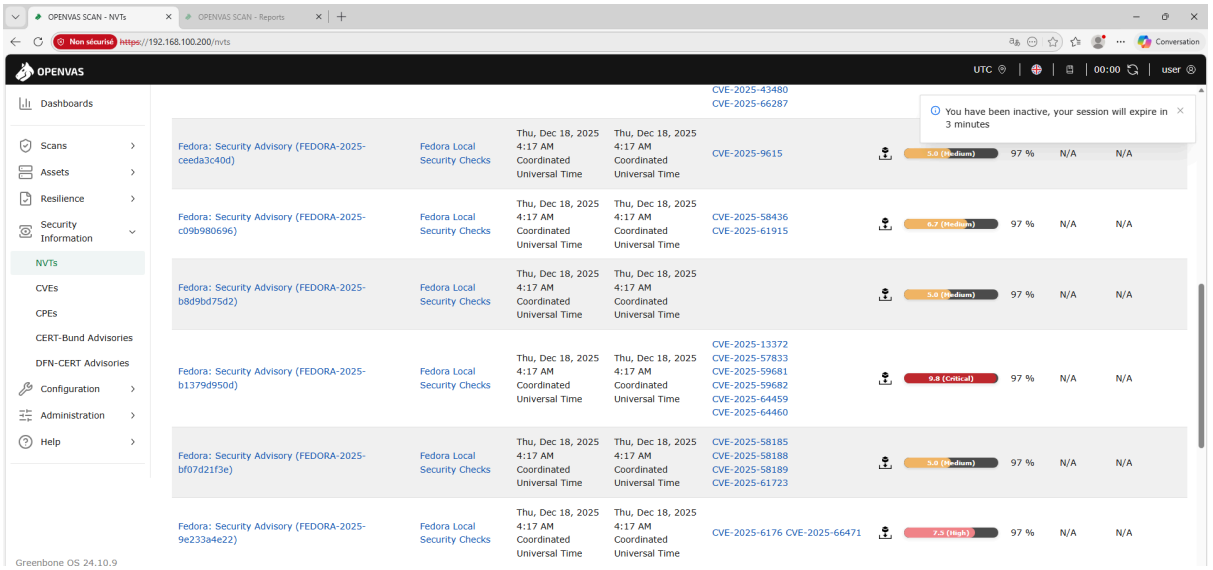
Consultation des NVTs (Network Vulnerability Tests) utilisés par OpenVAS pour détecter les vulnérabilités.



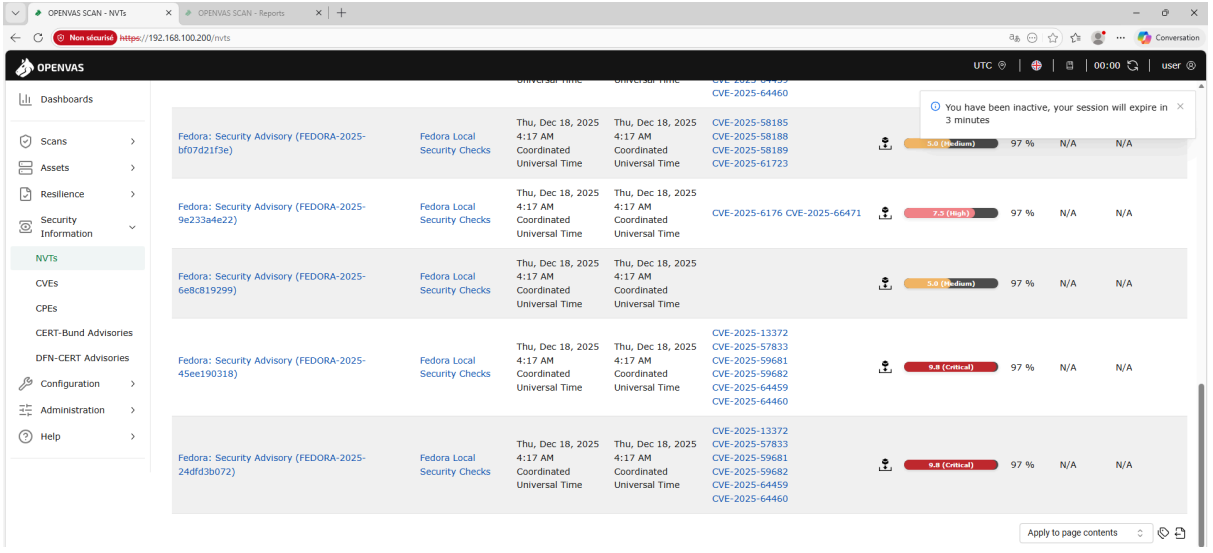
Affichage détaillé des signatures de vulnérabilités et des CVE associées détectées pendant le scan.



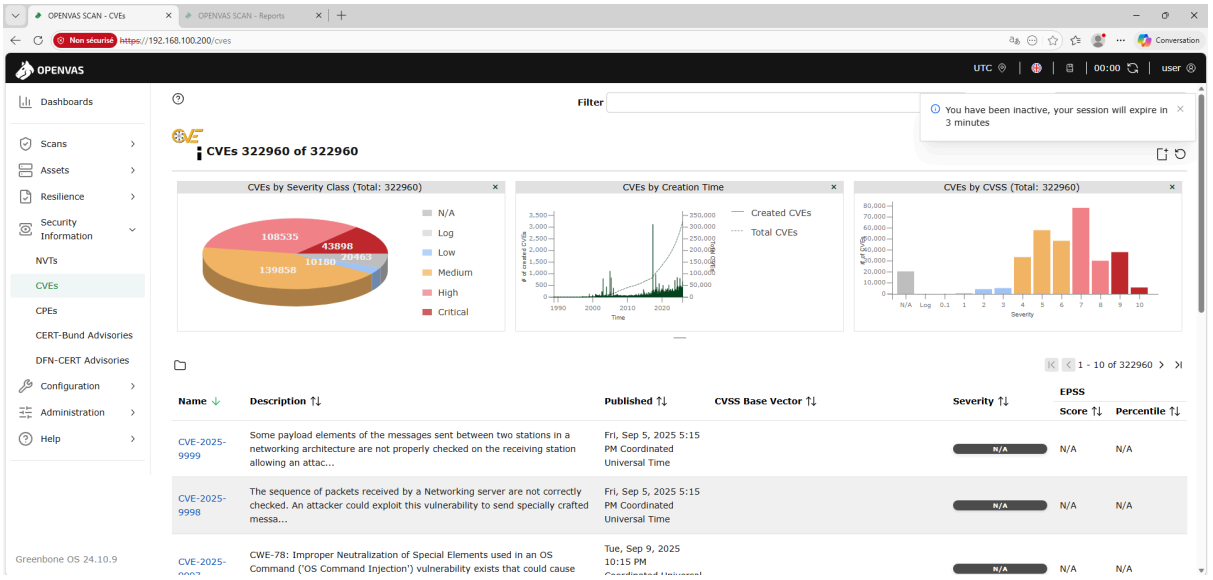
Consultation des avis de sécurité et des vulnérabilités référencées dans les bases NVT de Greenbone.



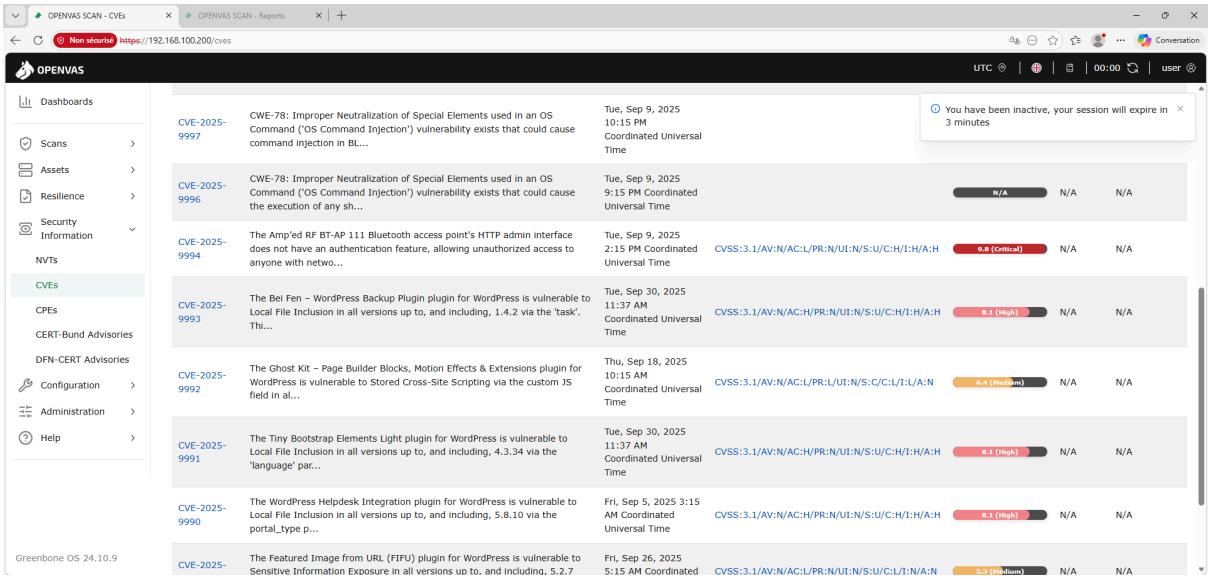
Analyse détaillée des CVE et des niveaux de sévérité détectés lors du scan de sécurité.



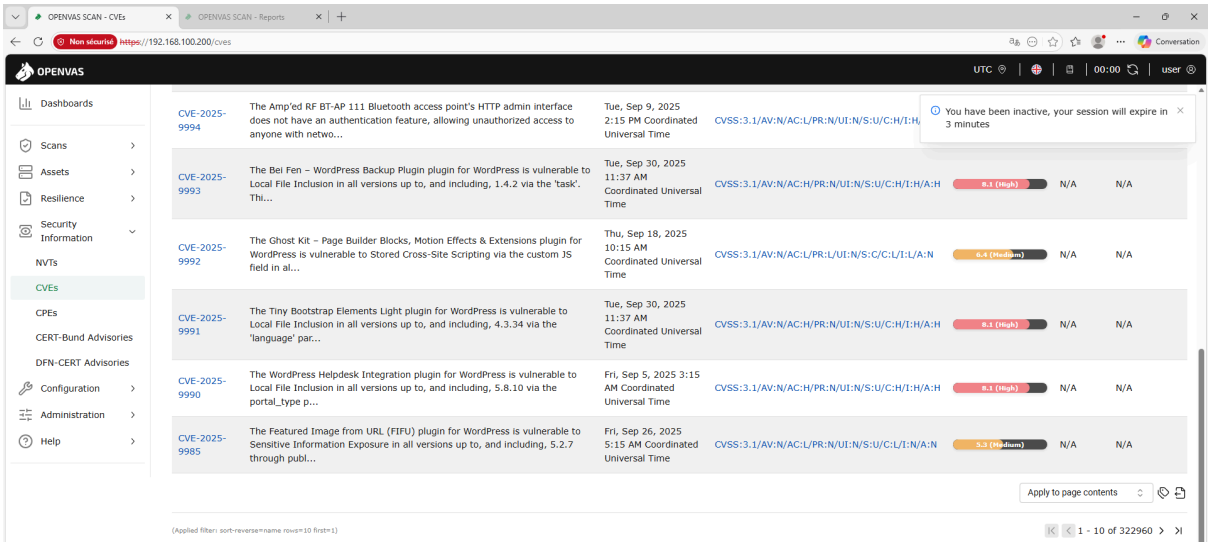
Affichage de la liste des CVE détectées avec leur répartition par niveau de sévérité.



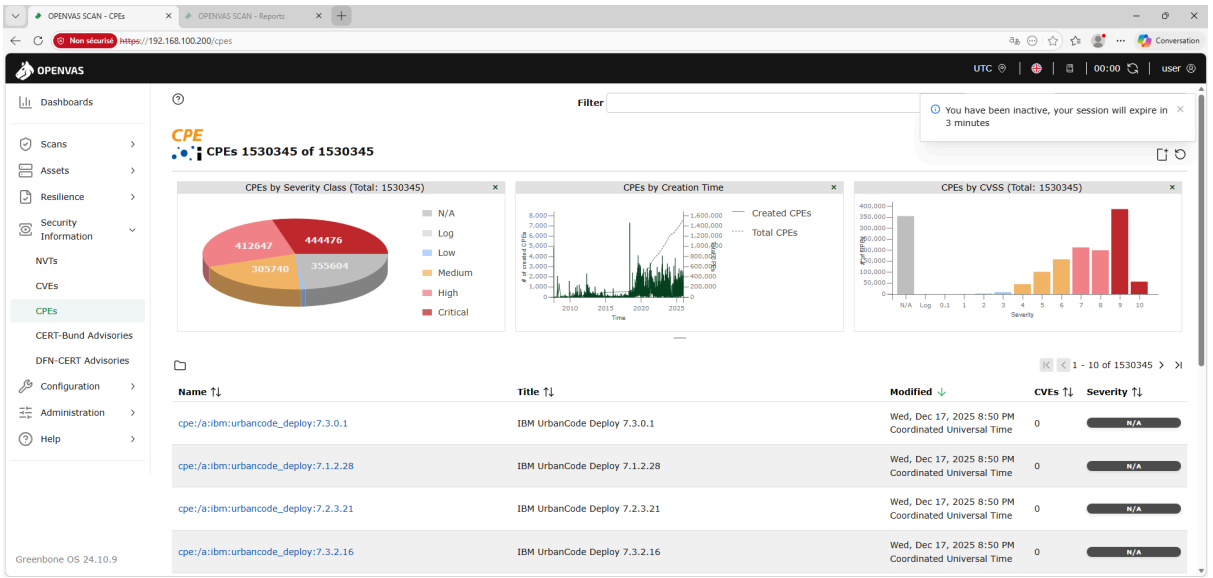
Consultation détaillée des failles CVE identifiées et des scores de criticité associés.



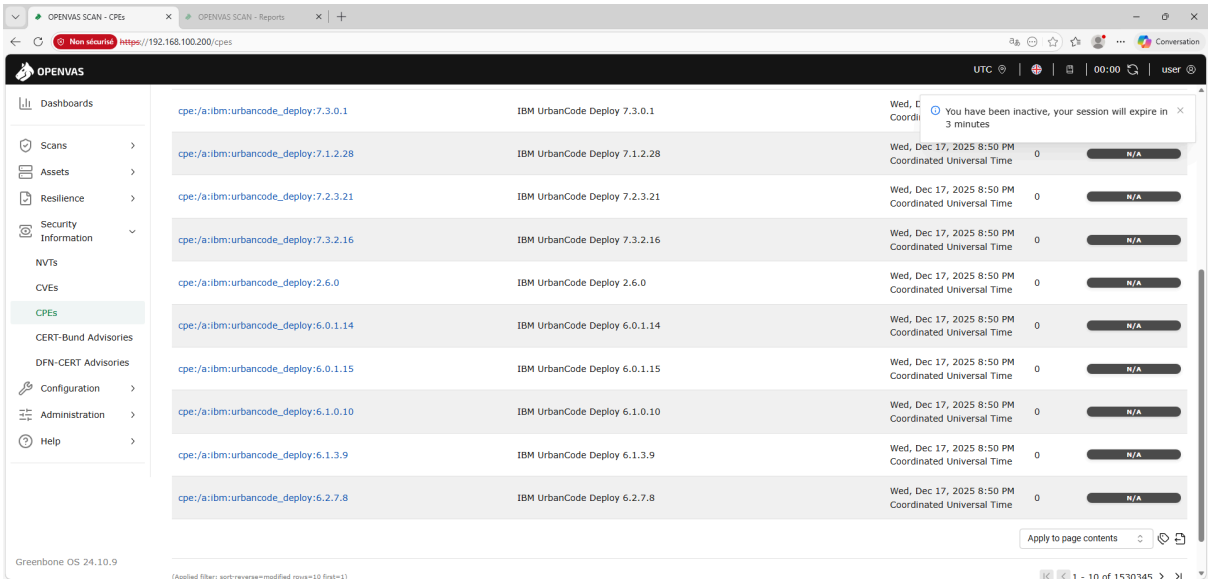
Analyse complémentaire des vulnérabilités CVE détectées par OpenVAS sur la machine cible.



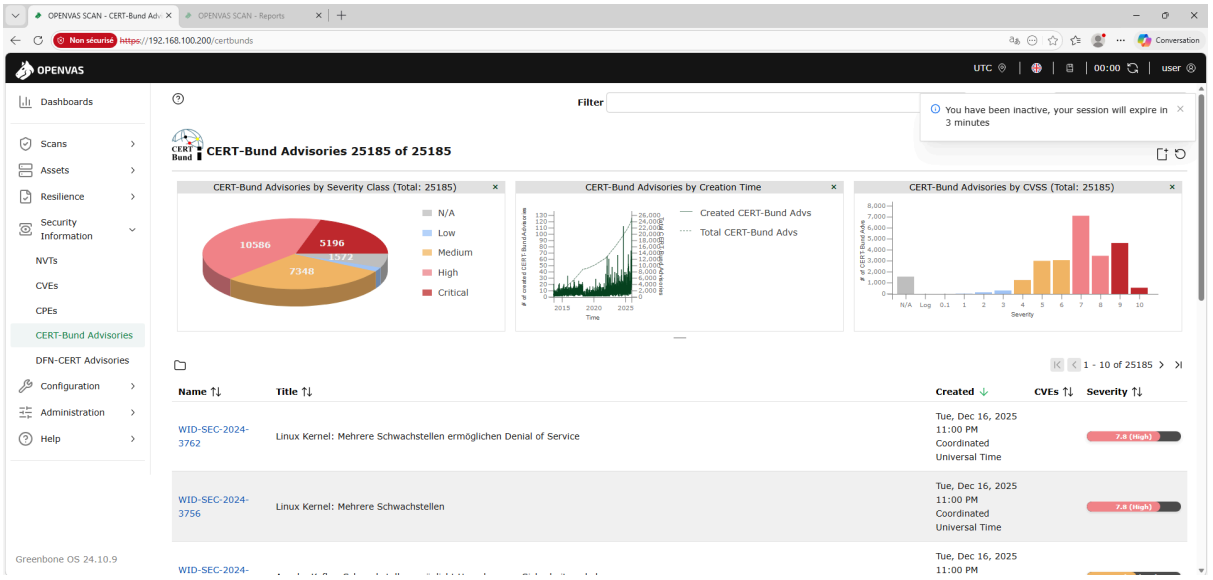
Consultation des CPE (Common Platform Enumeration) permettant d'identifier les logiciels et versions détectés sur la machine analysée.



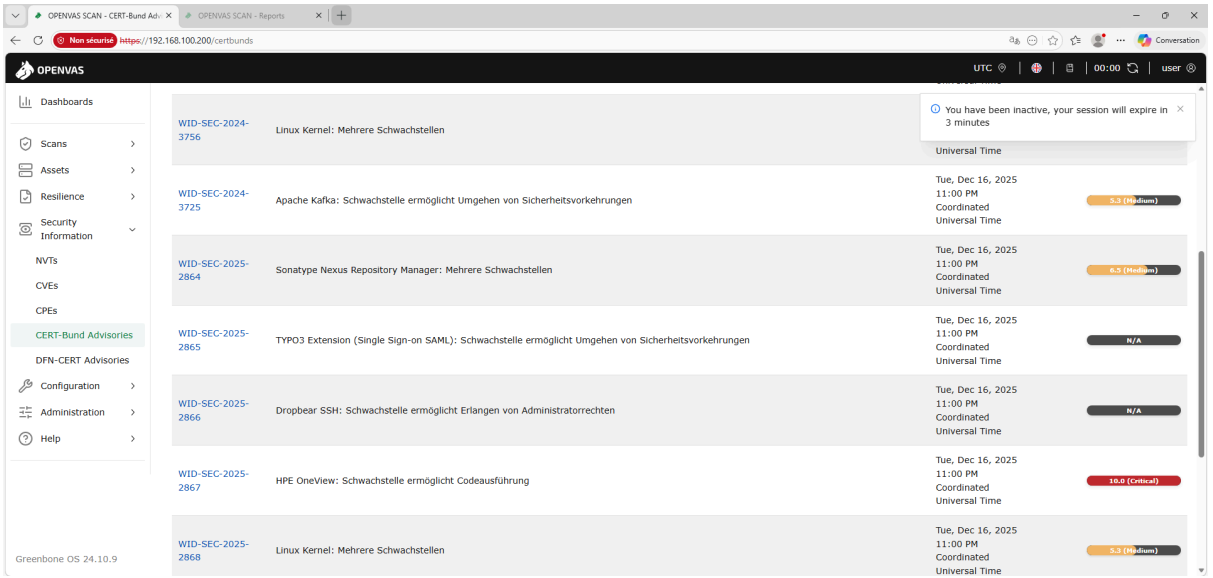
Affichage détaillé des logiciels détectés via les identifiants CPE pendant le scan OpenVAS.



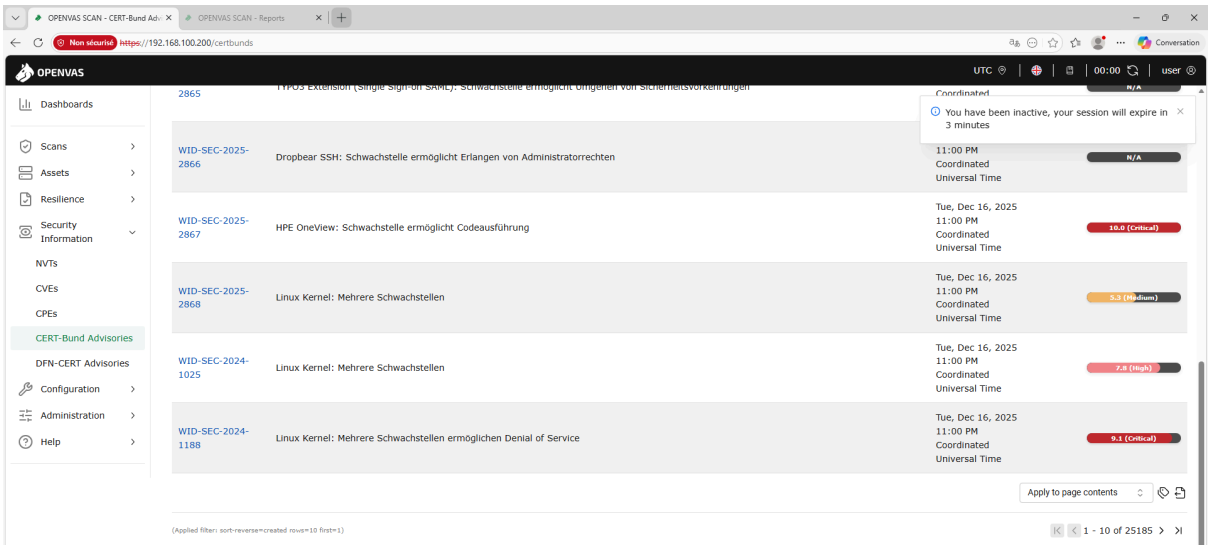
Consultation des avis CERT-Bund liés aux vulnérabilités détectées sur la machine analysée.



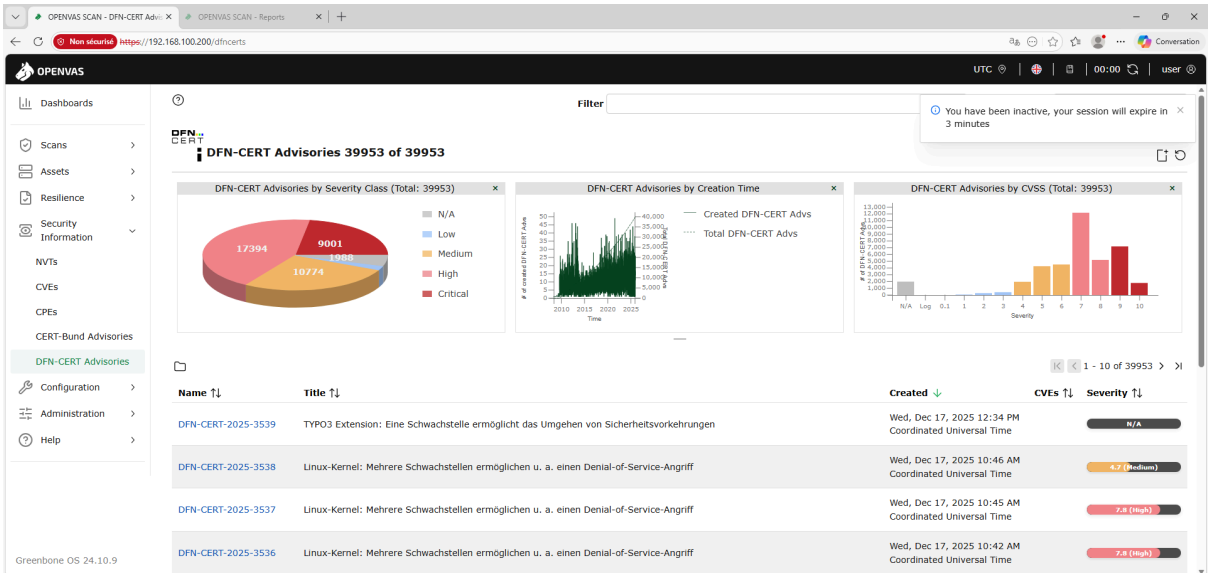
Affichage détaillé des avis CERT-Bund et des niveaux de sévérité associés aux vulnérabilités détectées.



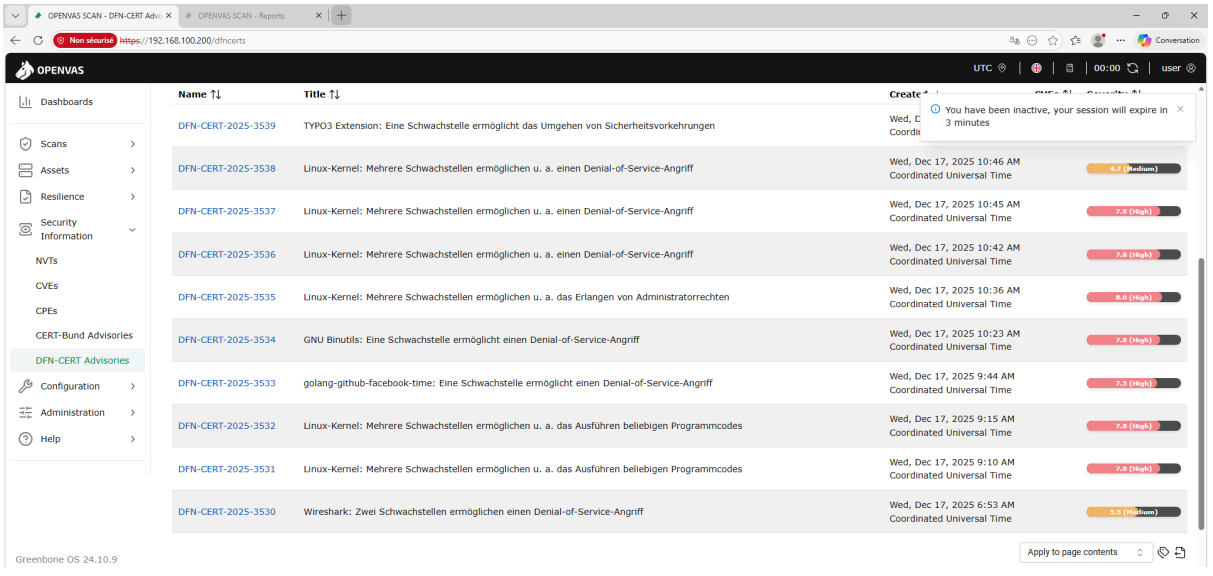
Consultation des recommandations de sécurité publiées par les organismes CERT concernant les failles identifiées.



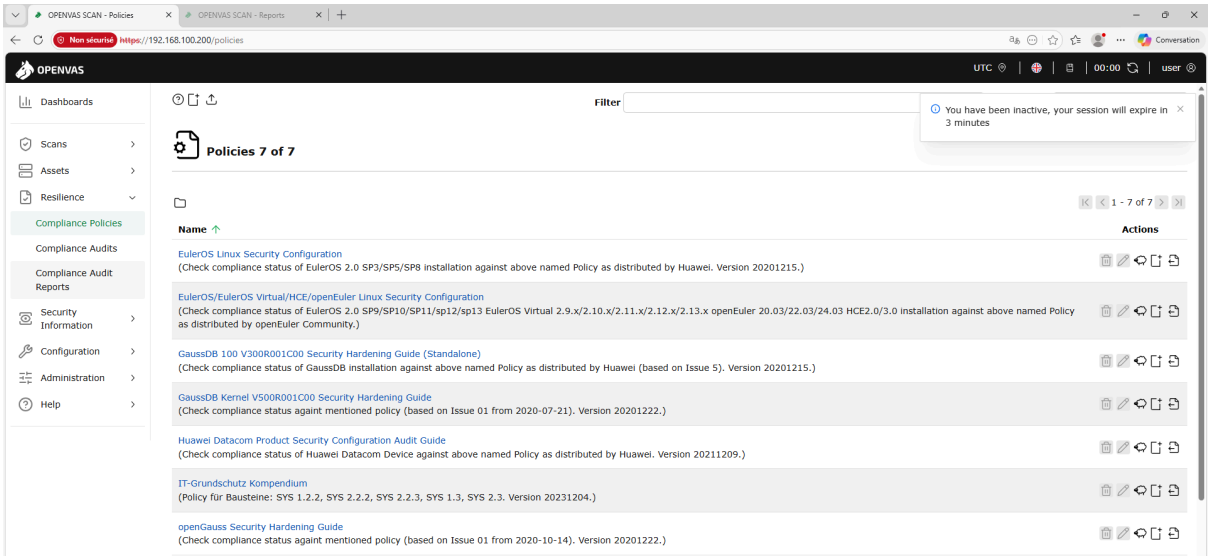
Consultation des avis DFN-CERT liés aux vulnérabilités détectées par OpenVAS.



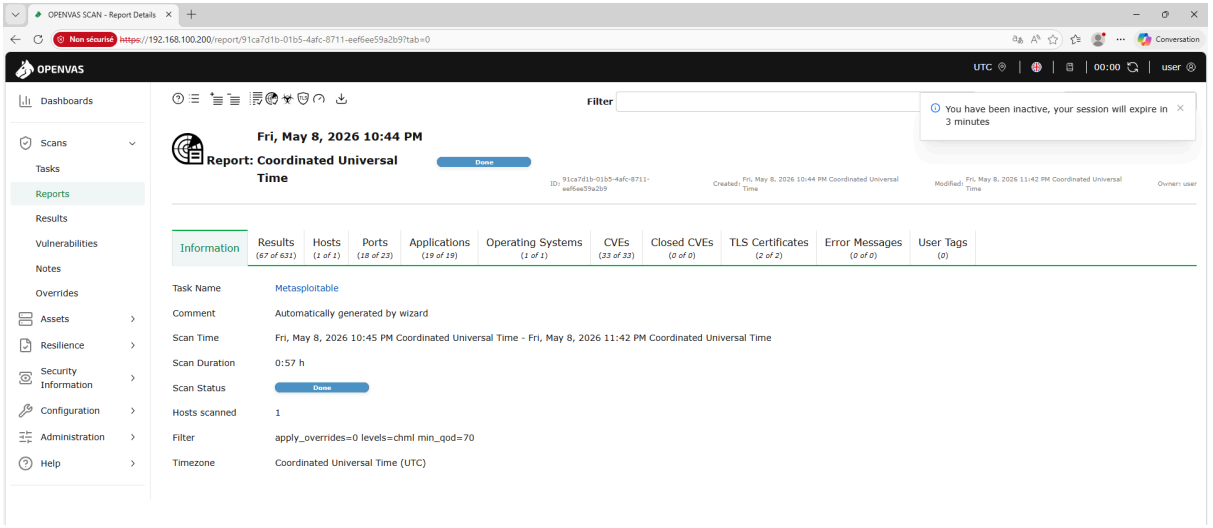
Analyse détaillée des alertes DFN-CERT et des niveaux de criticité associés aux failles de sécurité identifiées.



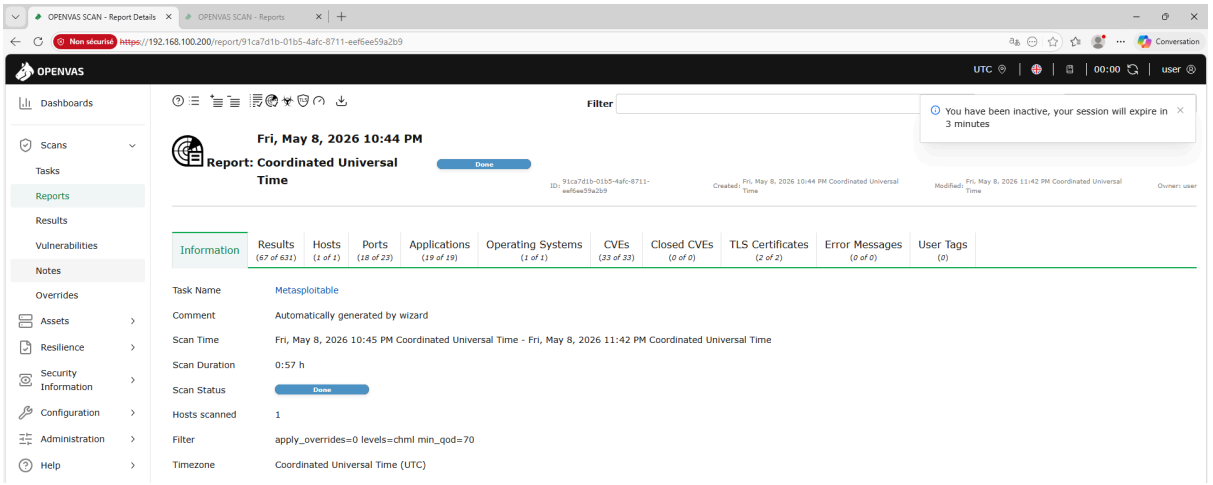
Consultation des politiques de conformité et des modèles d'audit de sécurité disponibles dans OpenVAS.



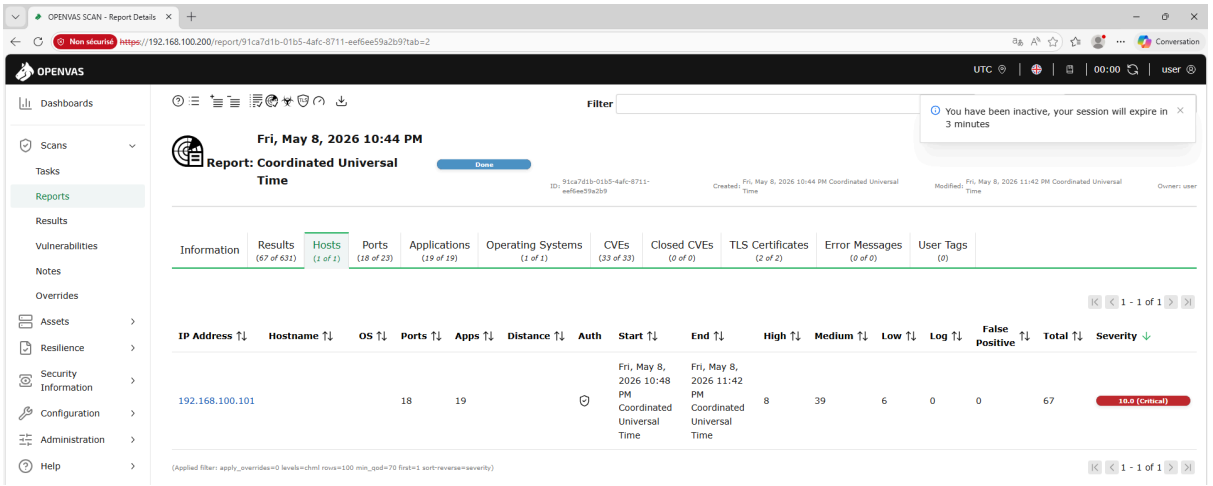
Affichage du rapport général du scan contenant les informations principales de l'analyse de vulnérabilités.



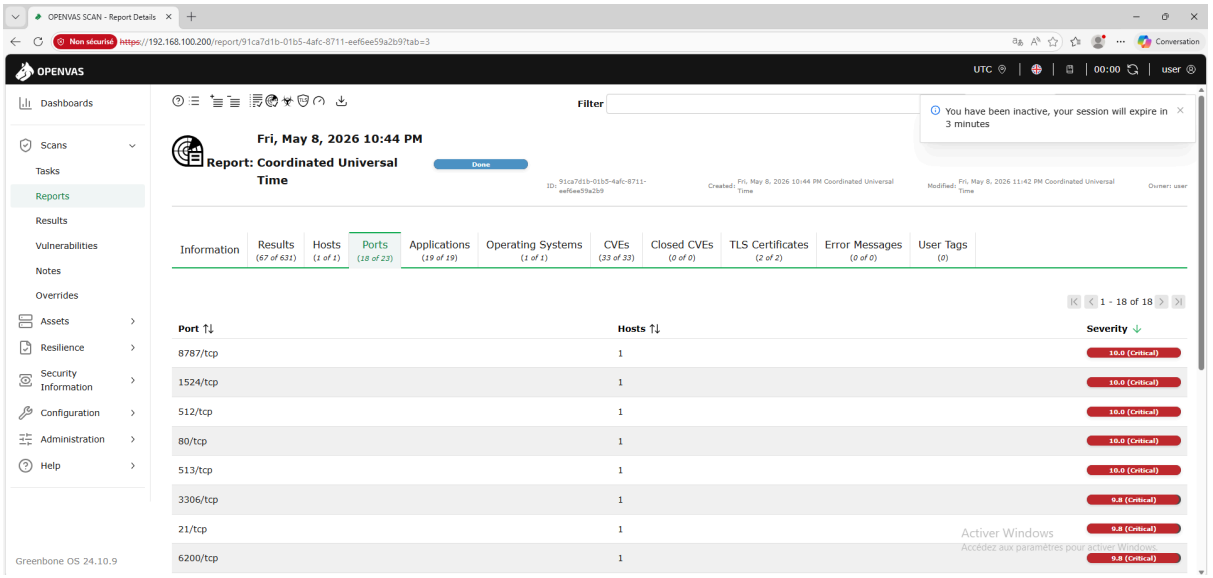
Consultation des informations générales du rapport de scan généré par OpenVAS.



Affichage du résumé des résultats du scan avec le nombre de vulnérabilités détectées et le score de sévérité global.

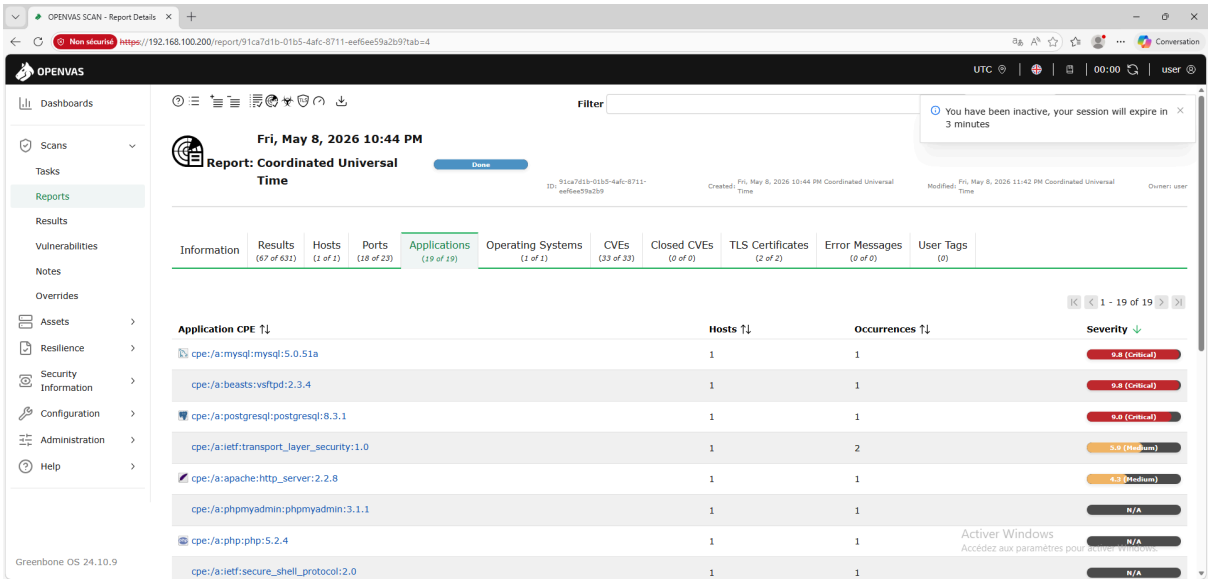


Consultation des ports ouverts détectés sur la machine analysée par OpenVAS.

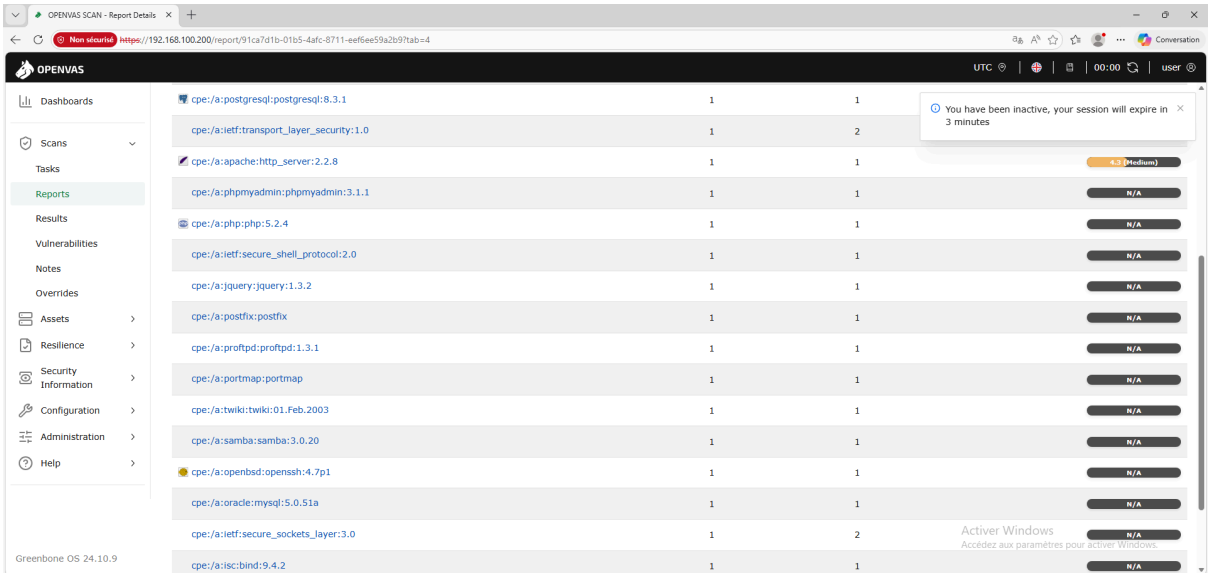


Analyse des services réseau exposés et des niveaux de sévérité associés aux ports détectés.

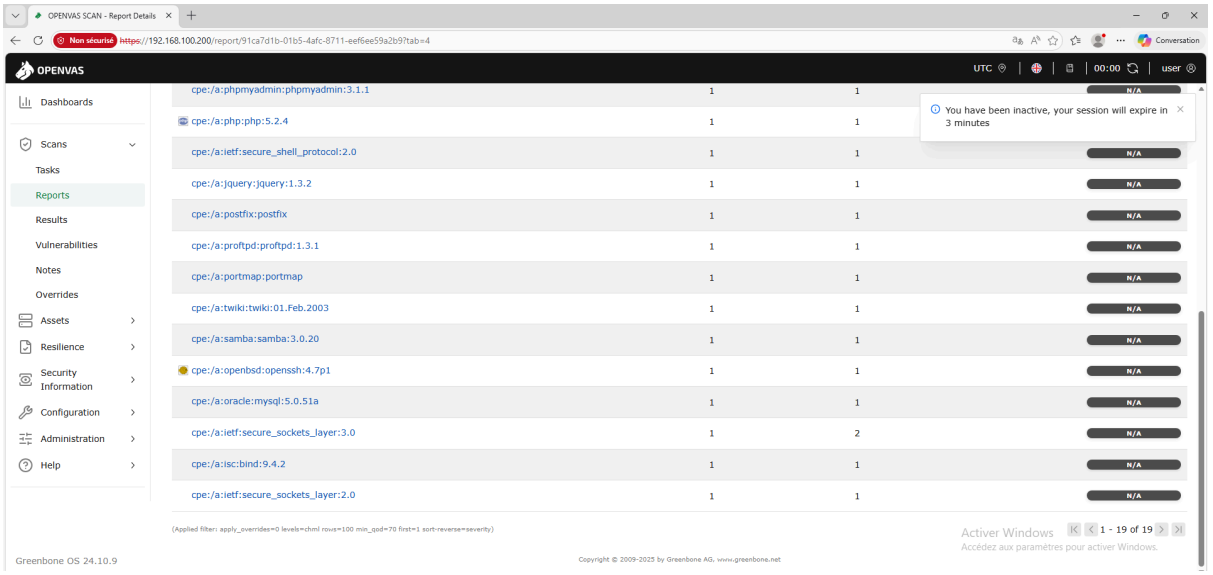
Consultation des applications détectées par OpenVAS sur la machine vulnérable analysée.



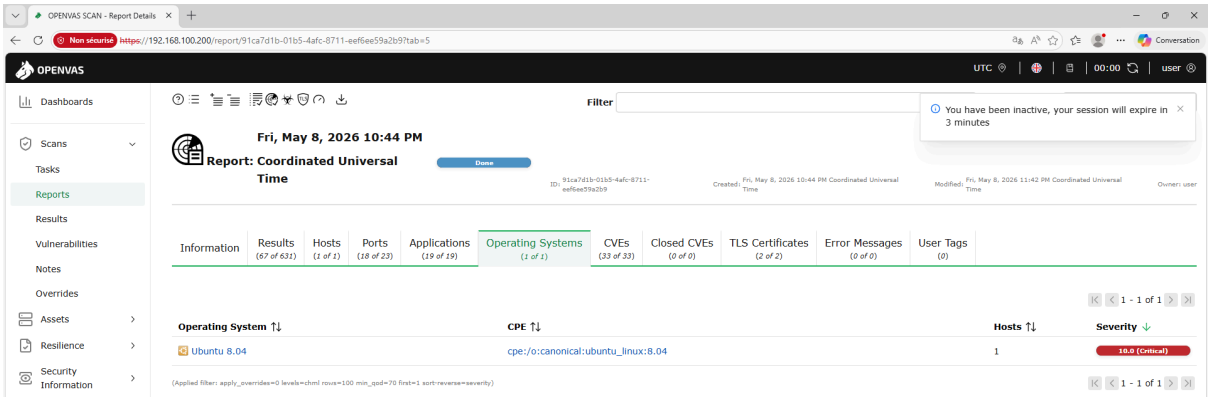
Analyse détaillée des logiciels et composants installés détectés pendant le scan de sécurité.



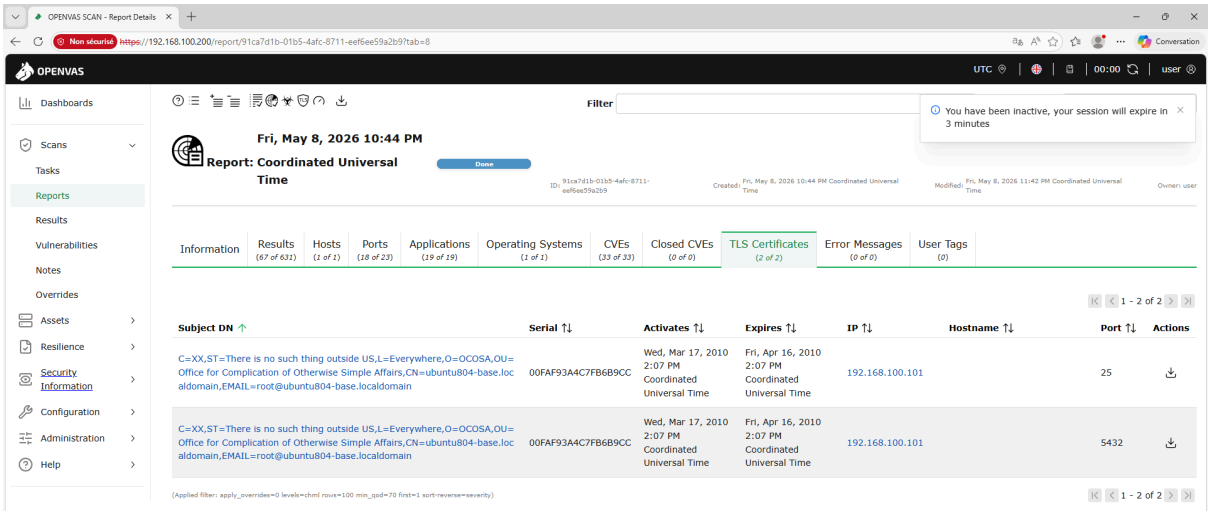
Fin de la liste des applications et composants détectés lors de l'analyse OpenVAS.



Identification du système d'exploitation détecté automatiquement sur la machine cible analysée.

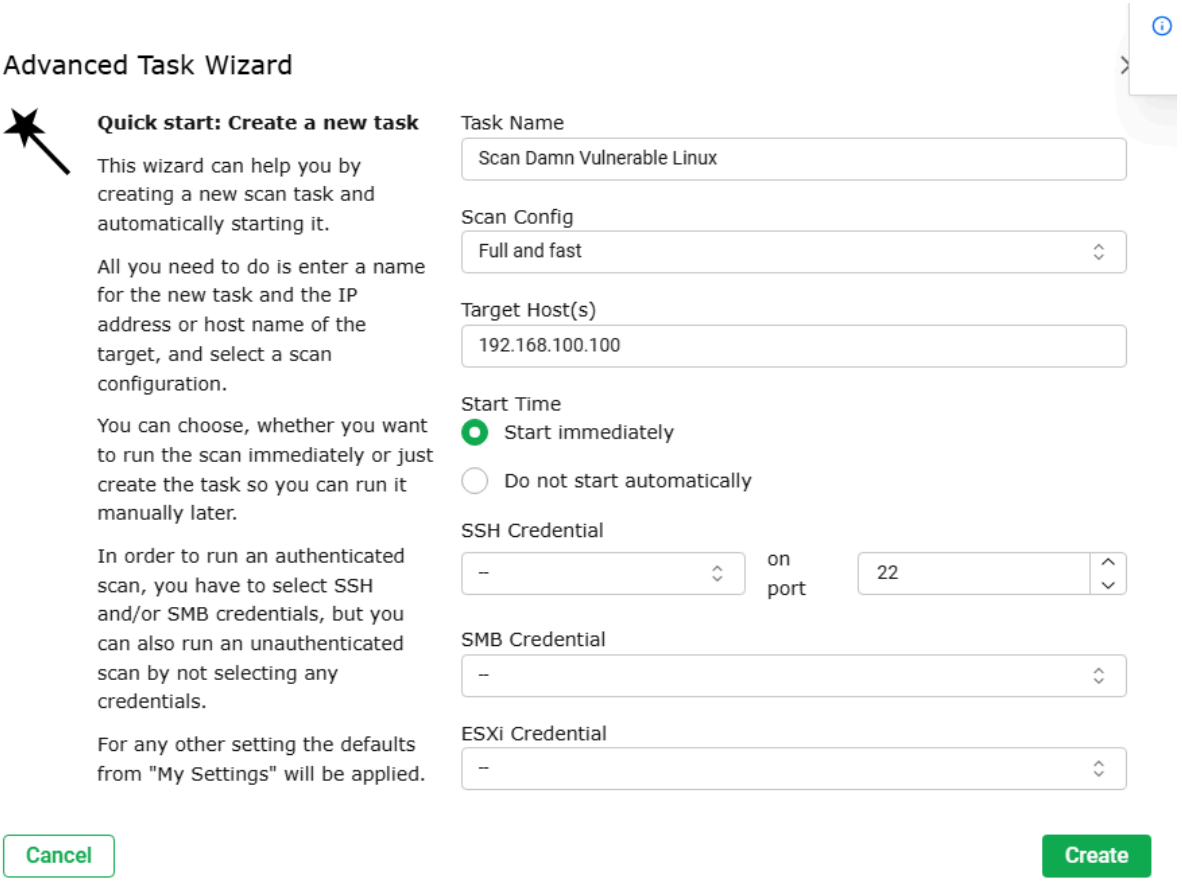


Consultation des certificats TLS détectés sur la machine cible pendant le scan OpenVAS.

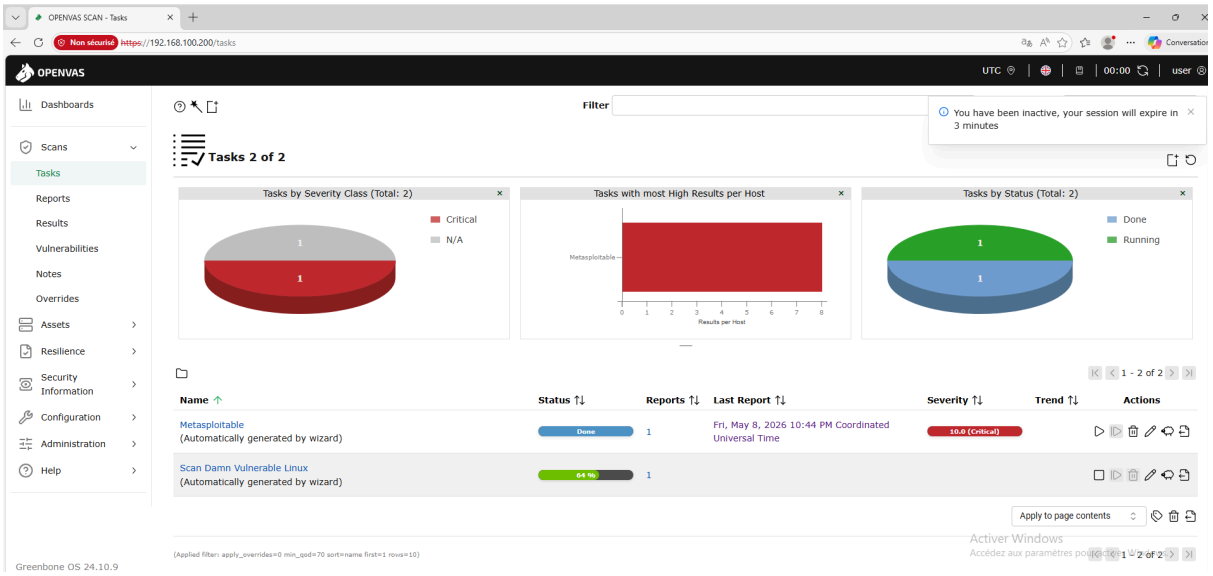


5. Test avec la VM Damn Vulnerable Linux

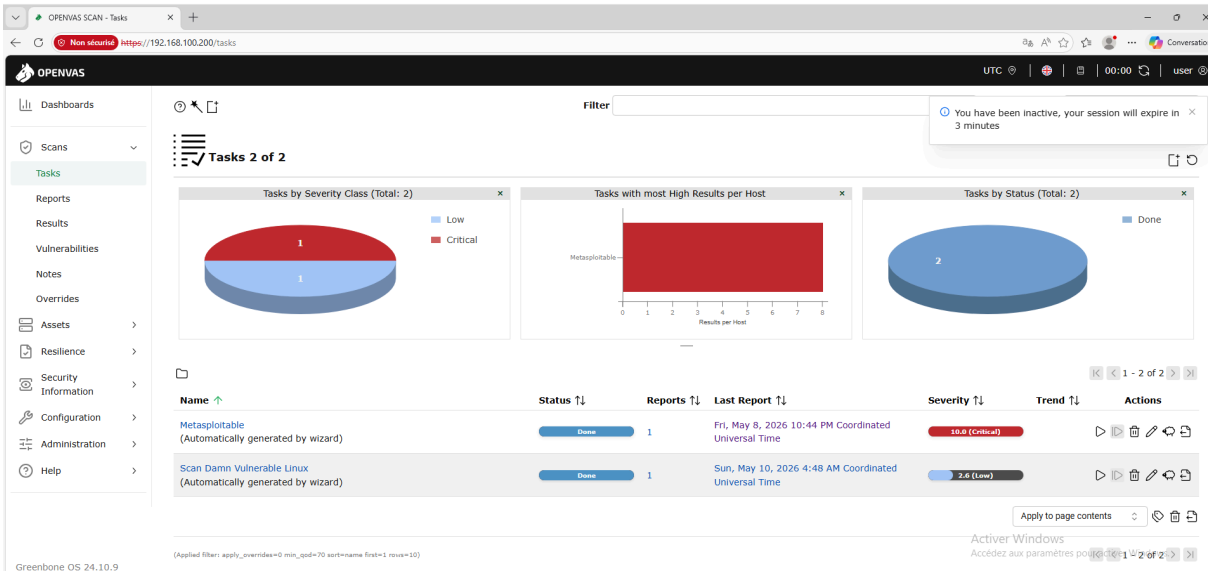
Création d'une tâche de scan OpenVAS pour analyser la machine Damn Vulnerable Linux avec le profil "Full and fast".



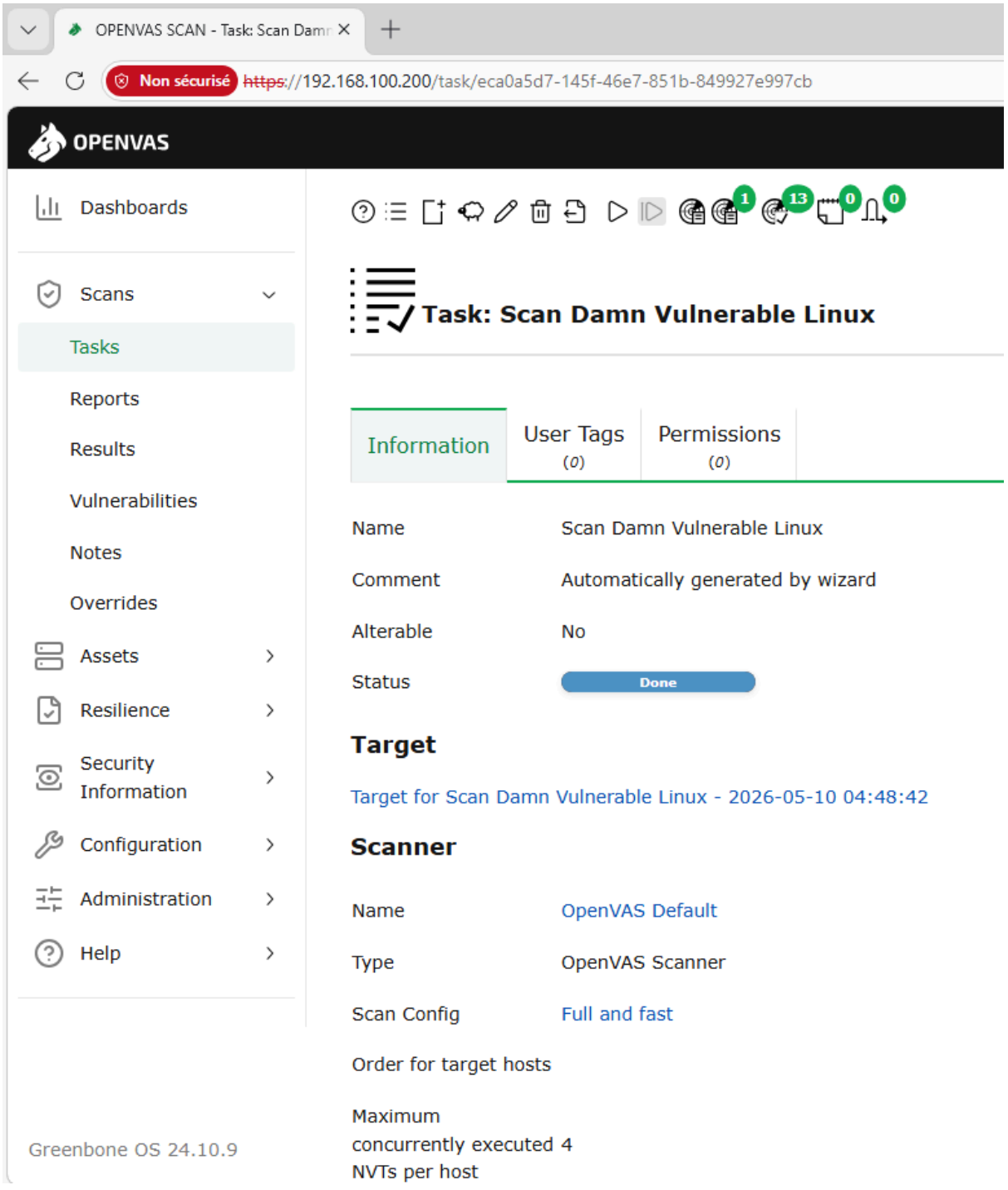
Lancement du scan de vulnérabilités sur la machine Damn Vulnerable Linux depuis OpenVAS.



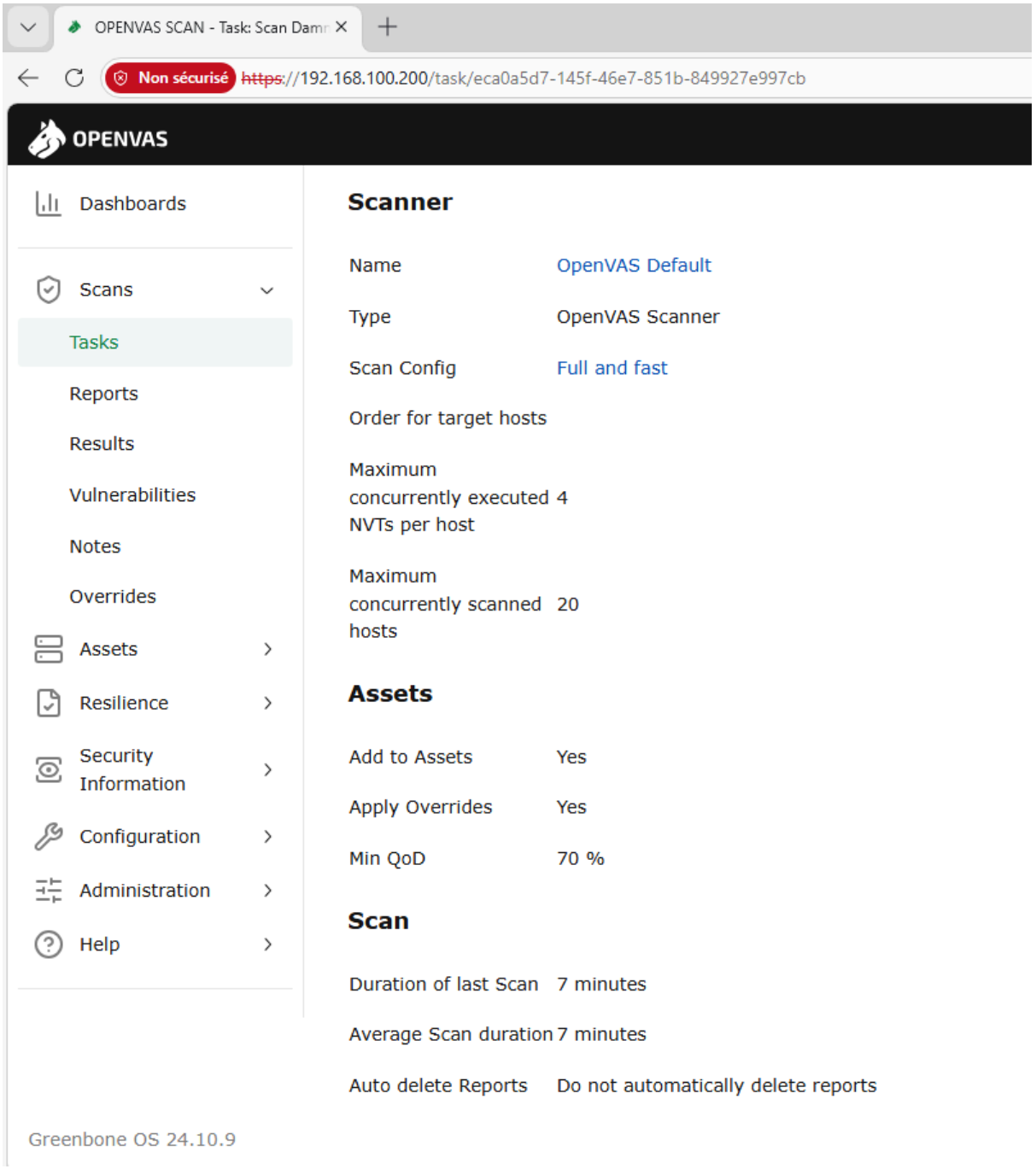
Consultation de l'état du scan après la fin de l'analyse de la machine Damn Vulnerable Linux.



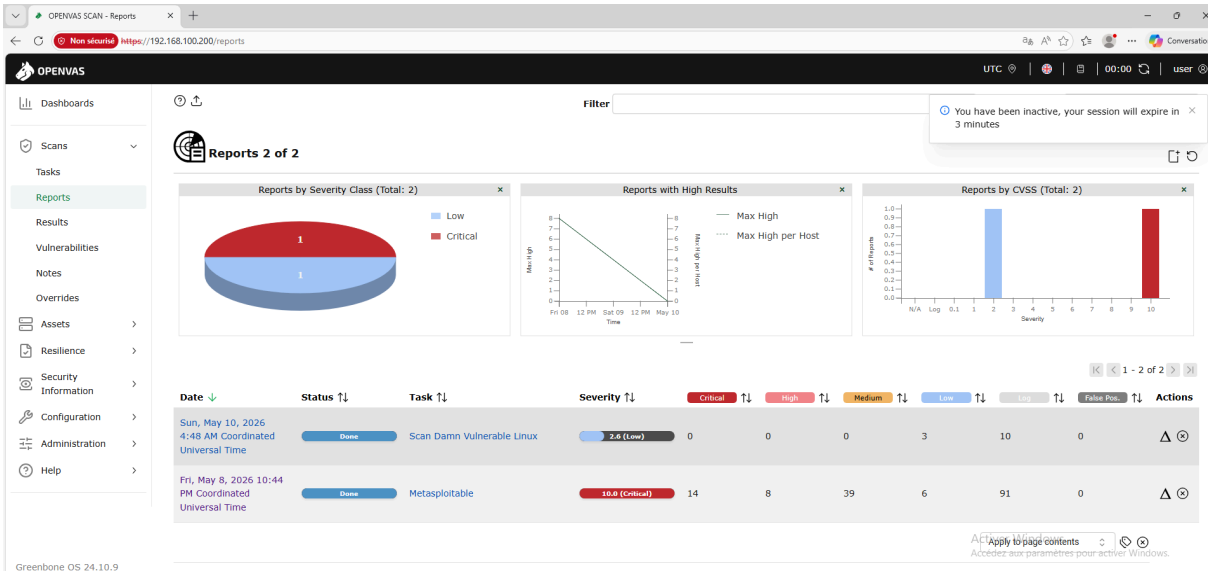
Affichage des informations générales de la tâche de scan Damn Vulnerable Linux dans OpenVAS.



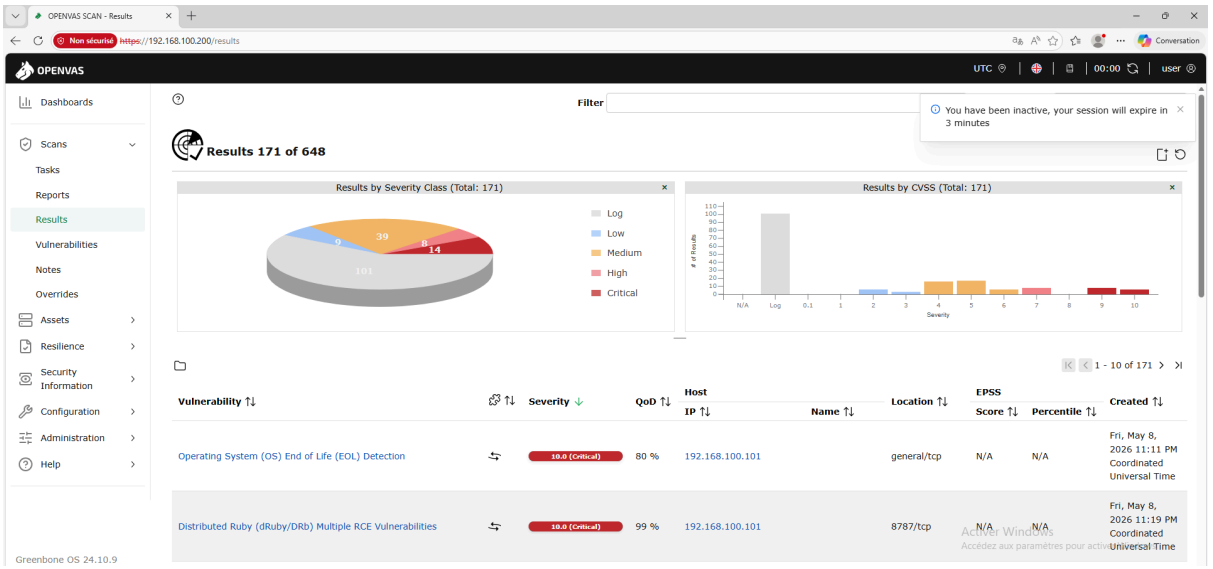
Consultation des paramètres du scanner OpenVAS et des informations de durée du scan effectué sur Damn Vulnerable Linux.



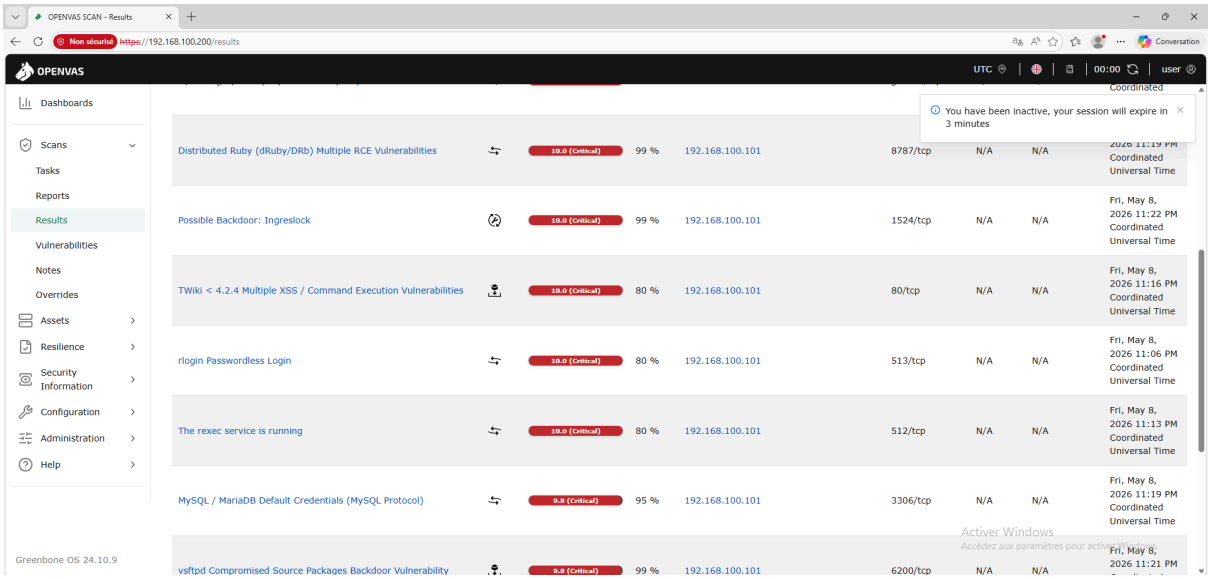
Consultation du rapport final du scan de la machine Damn Vulnerable Linux dans OpenVAS.



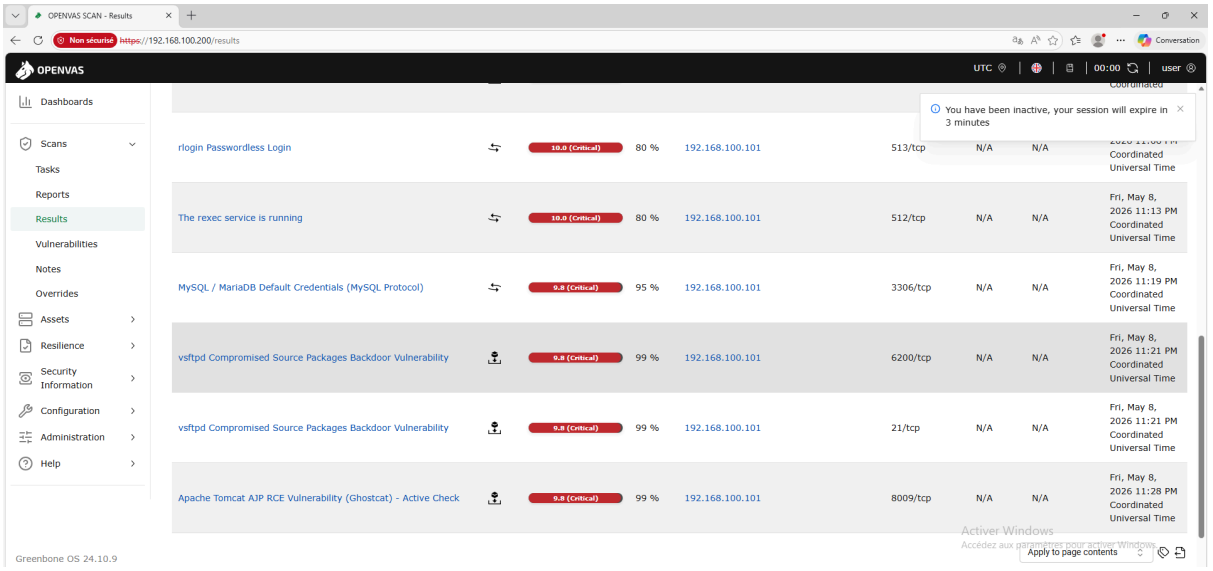
Affichage détaillé des résultats et des vulnérabilités détectées sur Damn Vulnerable Linux.



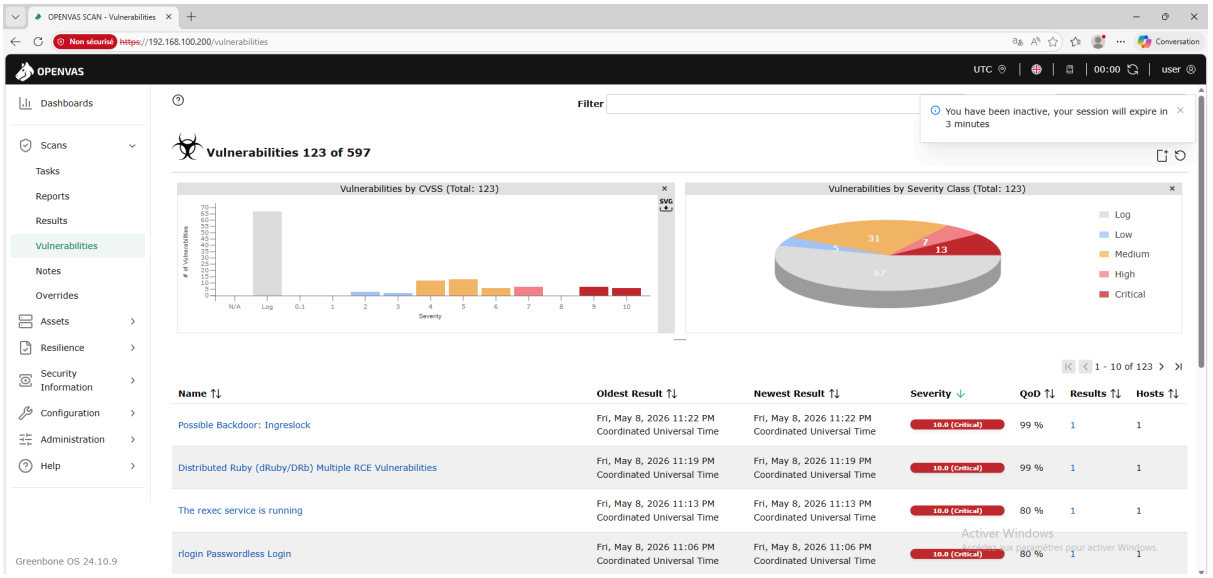
Consultation des vulnérabilités critiques détectées sur la machine Damn Vulnerable Linux.



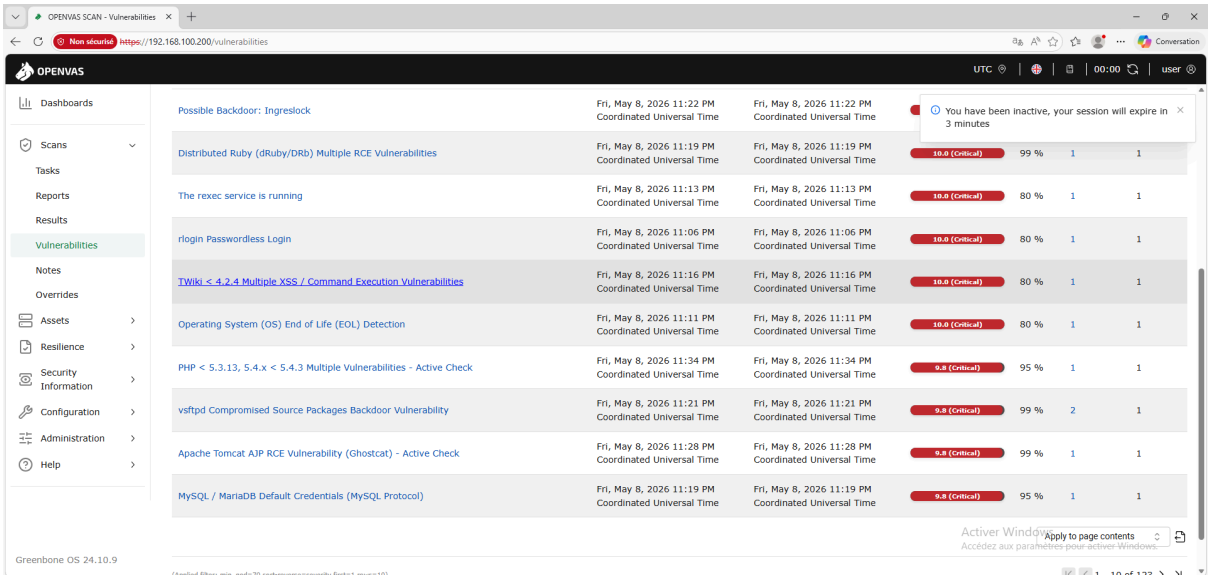
Analyse détaillée des failles de sécurité identifiées avec leurs niveaux de sévérité associés.



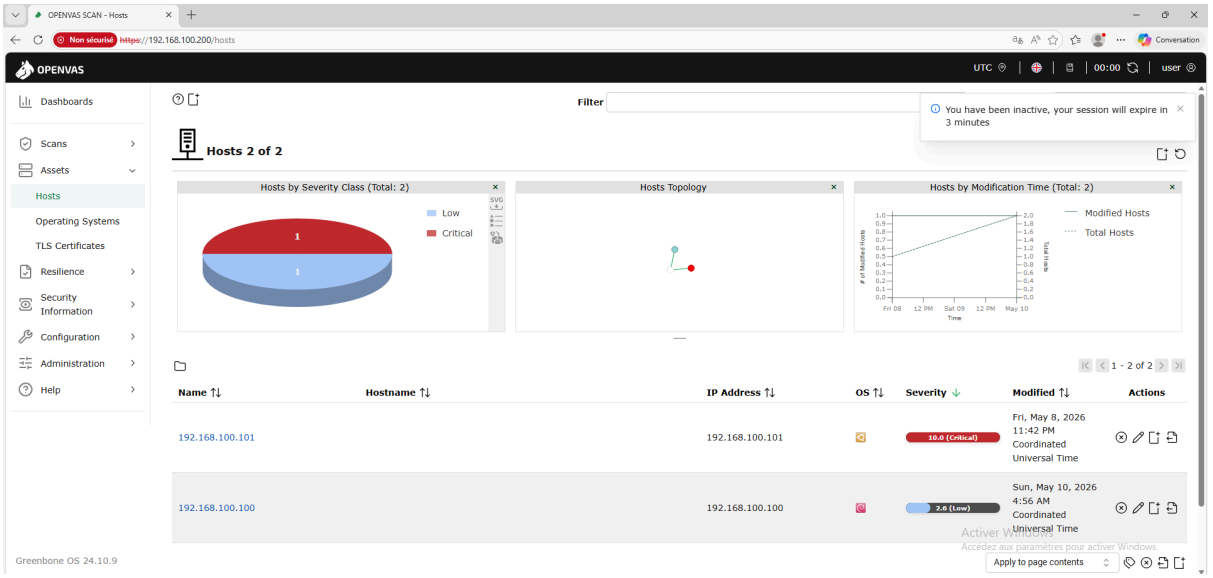
Affichage de la liste des vulnérabilités détectées sur Damn Vulnerable Linux avec leur niveau de criticité.



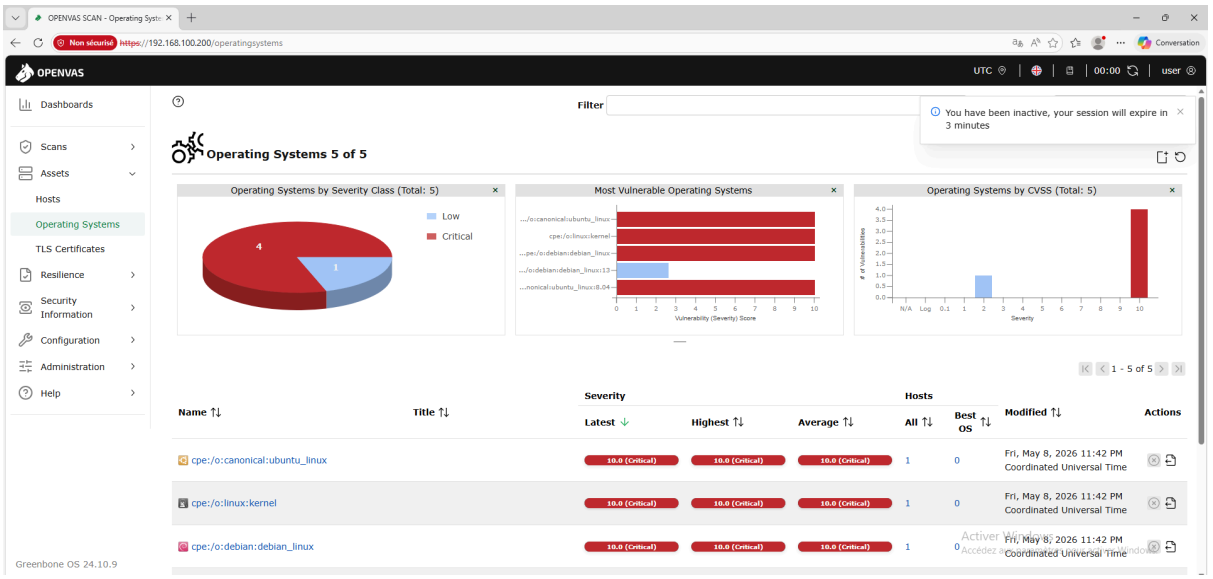
Analyse détaillée des failles de sécurité critiques présentes sur la machine cible analysée.



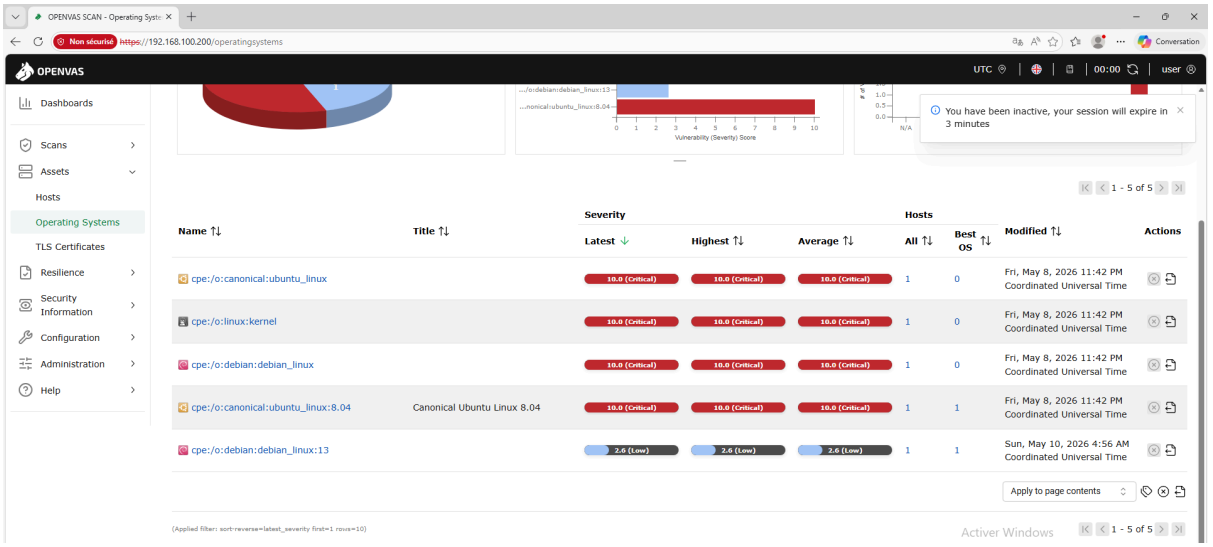
Consultation des hôtes détectés et des niveaux de sévérité associés après le scan de Damn Vulnerable Linux.



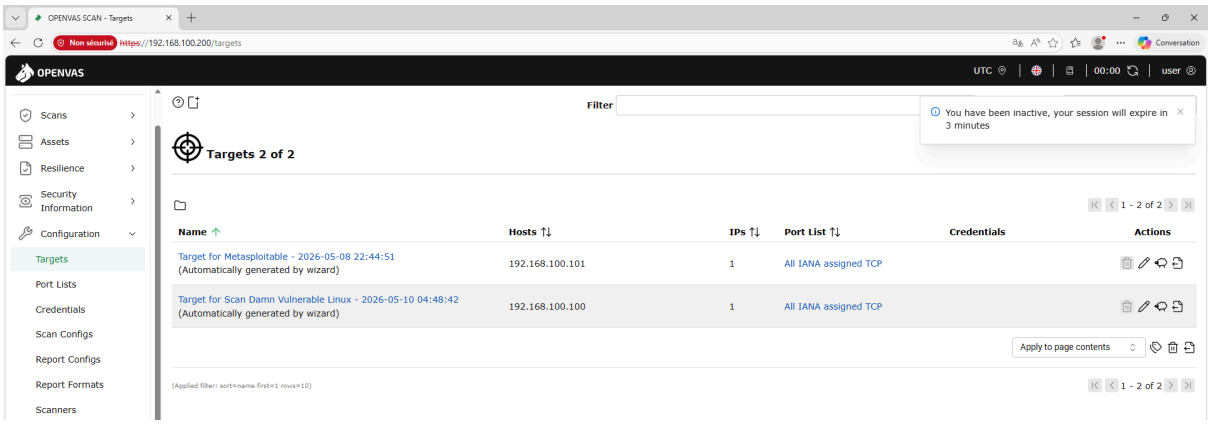
Identification des systèmes d'exploitation détectés automatiquement par OpenVAS lors de l'analyse.



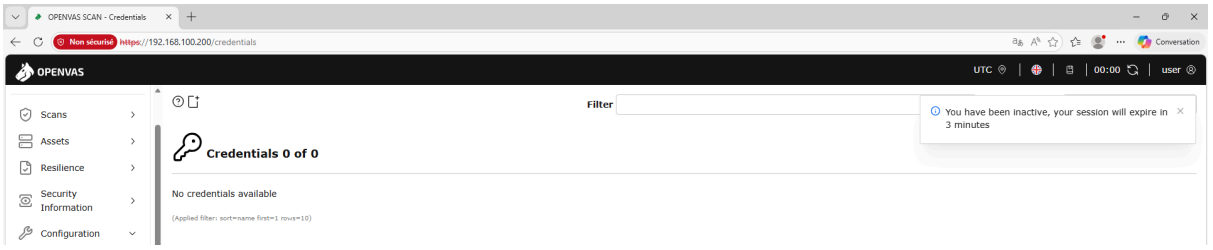
Affichage des systèmes d'exploitation détectés et des niveaux de criticité associés.



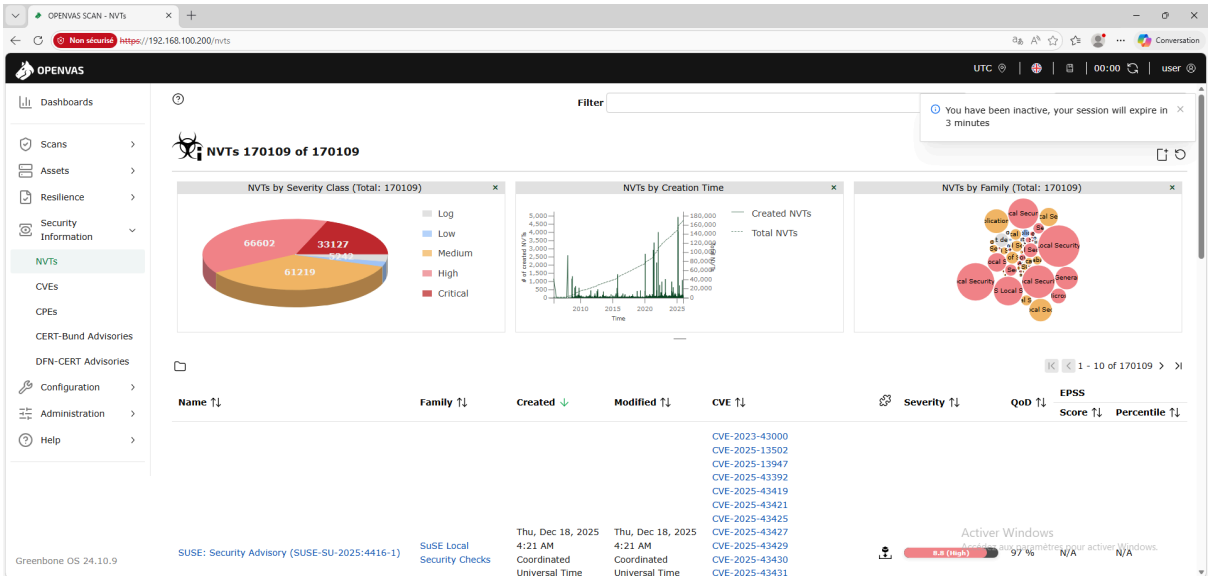
Consultation des différentes cibles configurées dans OpenVAS pour les scans de vulnérabilités.



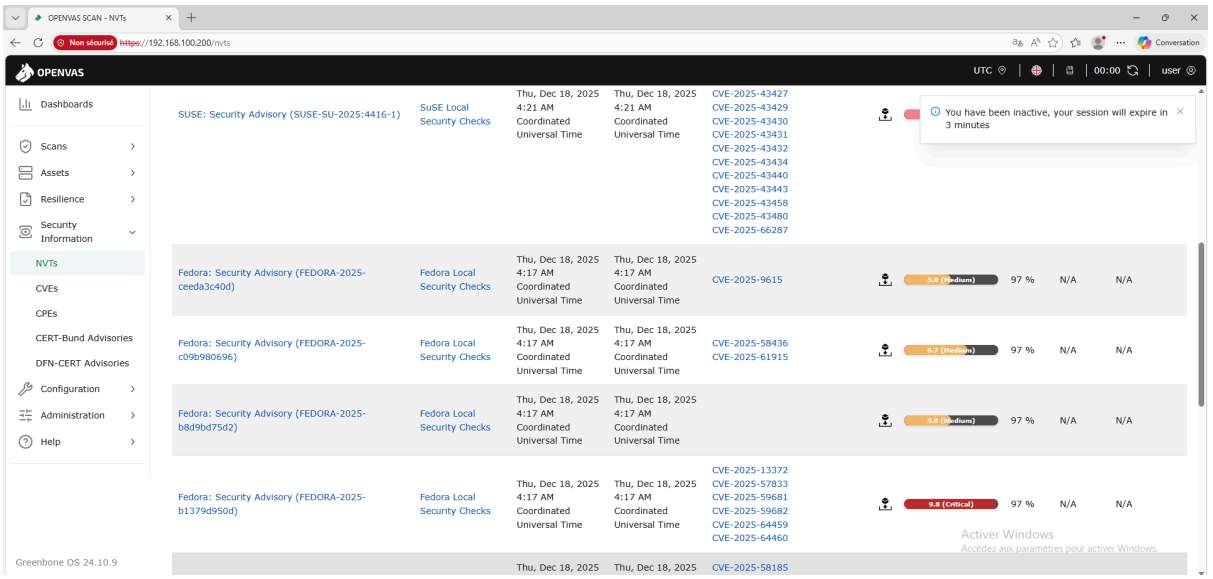
Vérification de l'absence d'identifiants configurés pour les scans authentifiés OpenVAS.



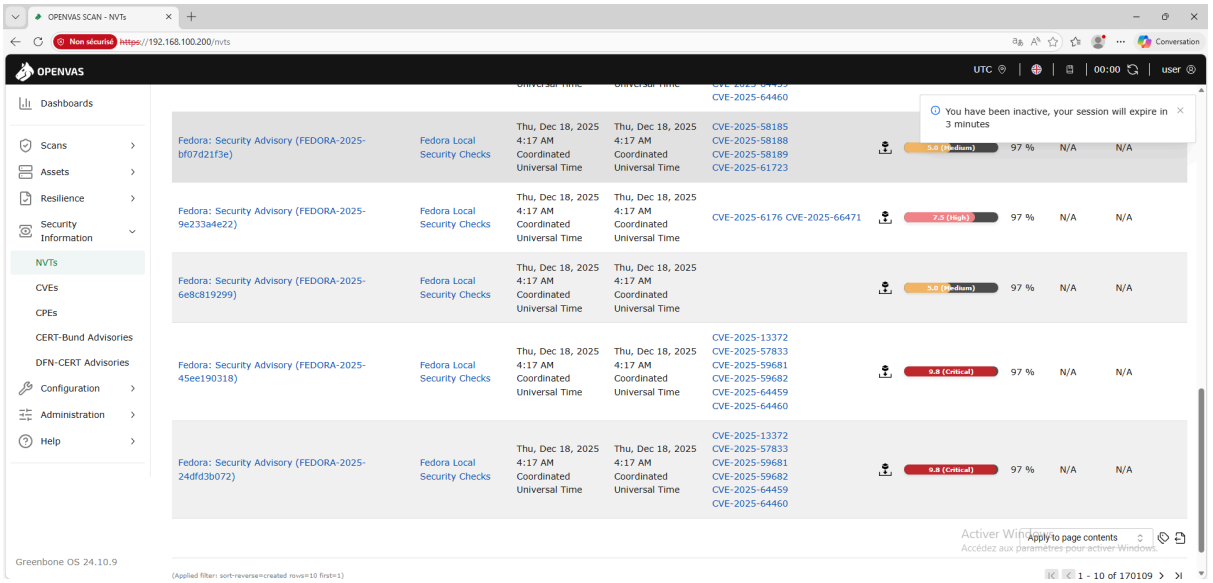
Consultation des NVT (Network Vulnerability Tests) utilisés pour détecter les vulnérabilités sur Damn Vulnerable Linux.



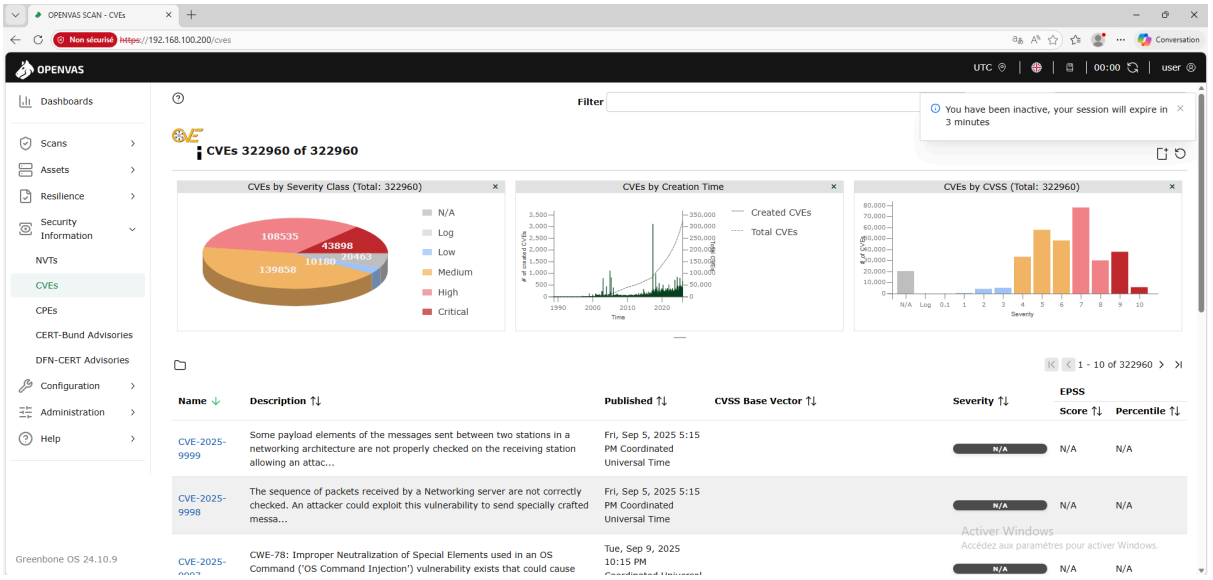
Analyse détaillée des signatures de vulnérabilités et des CVE associées détectées par OpenVAS.



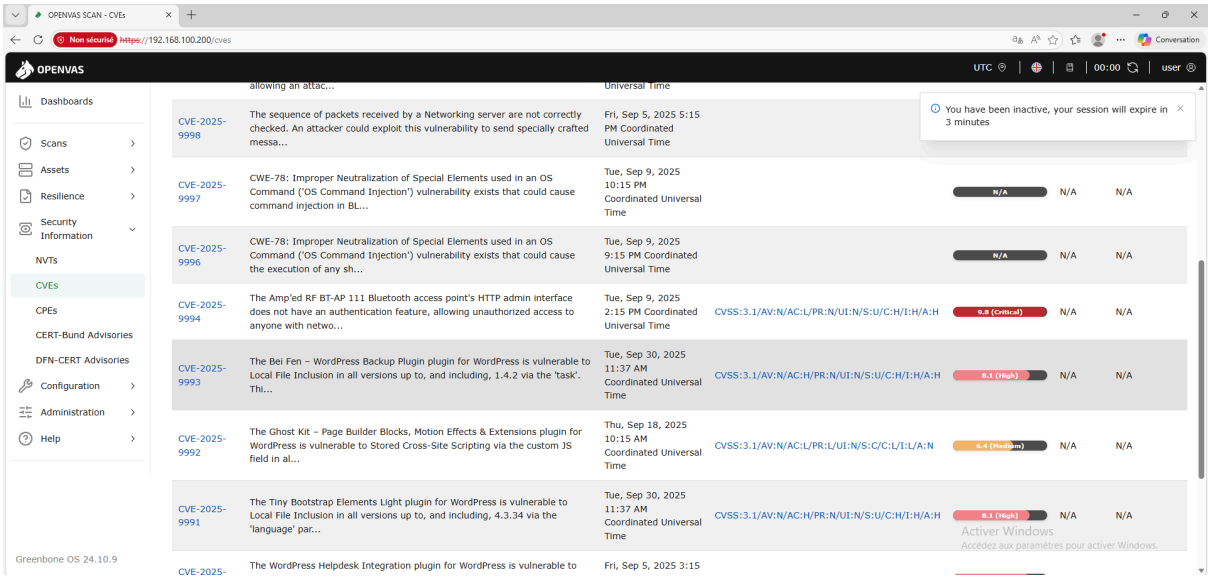
Affichage de la liste des CVE détectées avec leur niveau de sévérité sur la machine analysée.



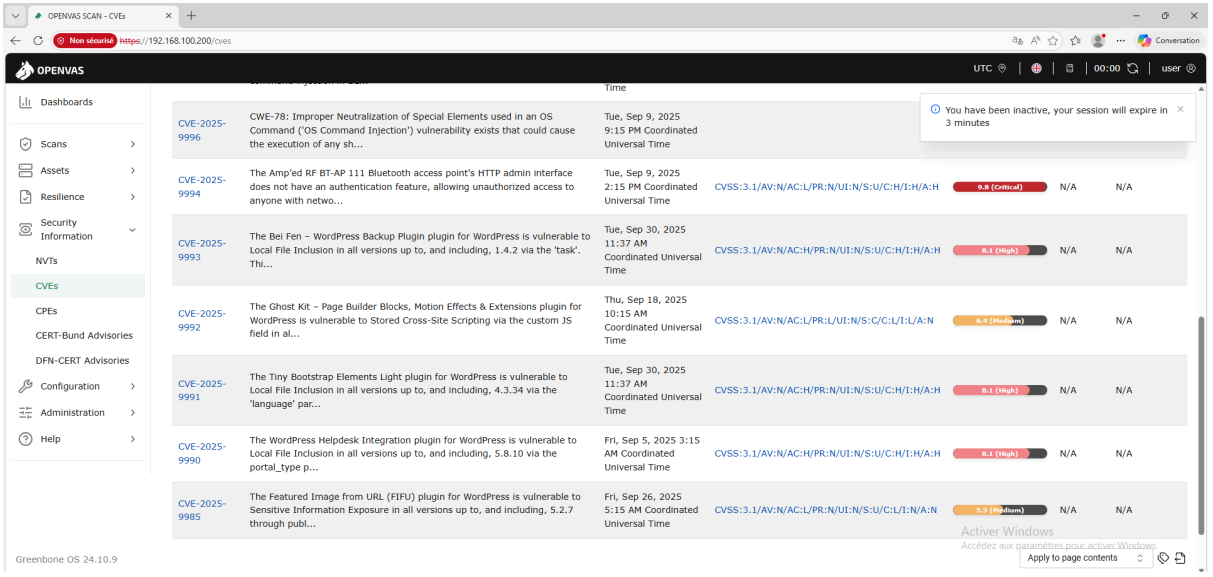
Consultation détaillée des failles CVE identifiées et des scores de criticité associés.



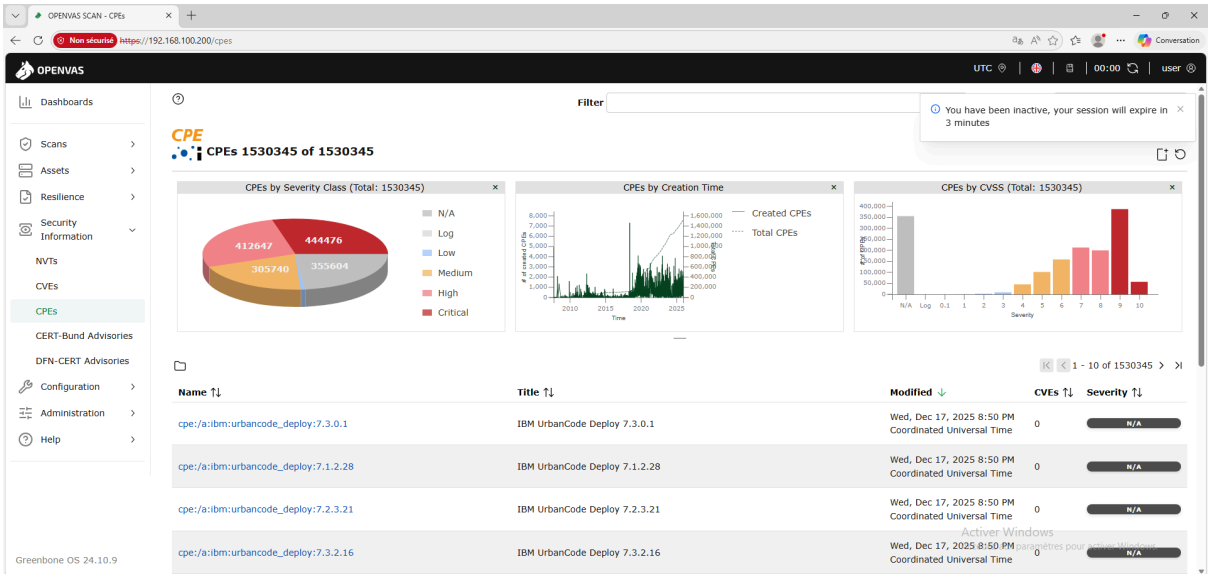
Affichage des logiciels et composants détectés via les identifiants CPE pendant le scan.



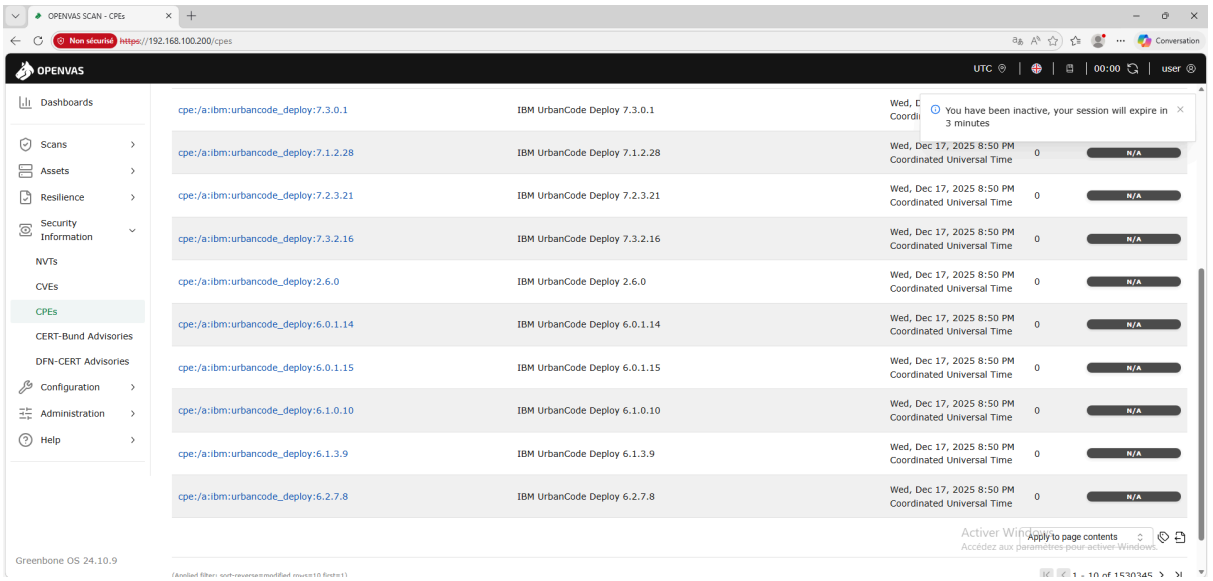
Analyse détaillée des applications détectées et des versions logicielles présentes sur la machine cible.



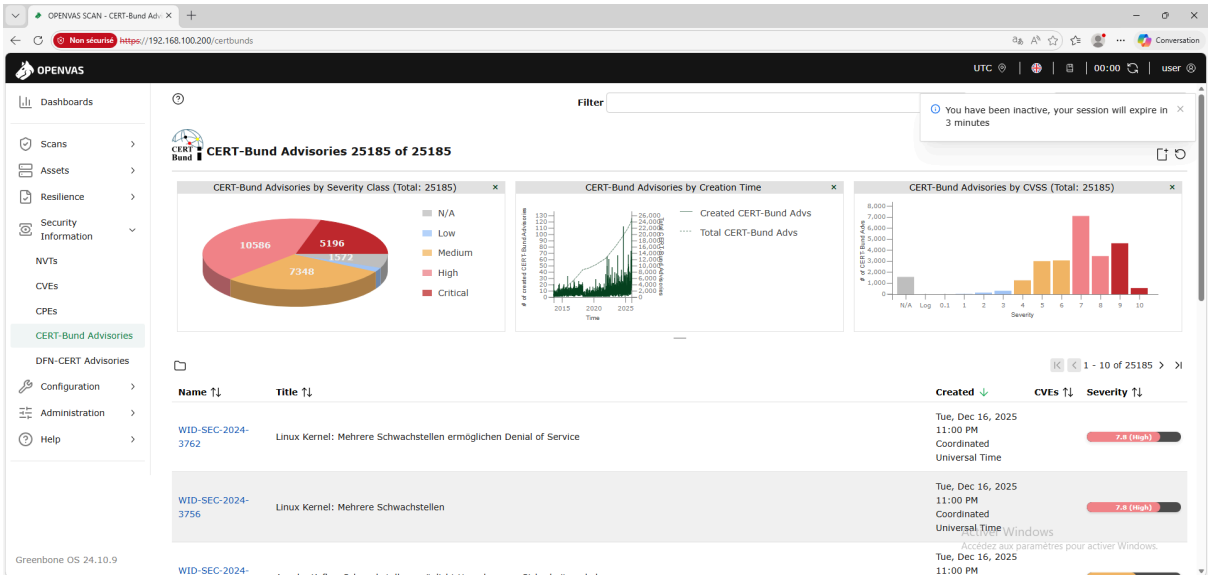
Consultation des avis CERT-Bund liés aux vulnérabilités détectées sur Damn Vulnerable Linux.



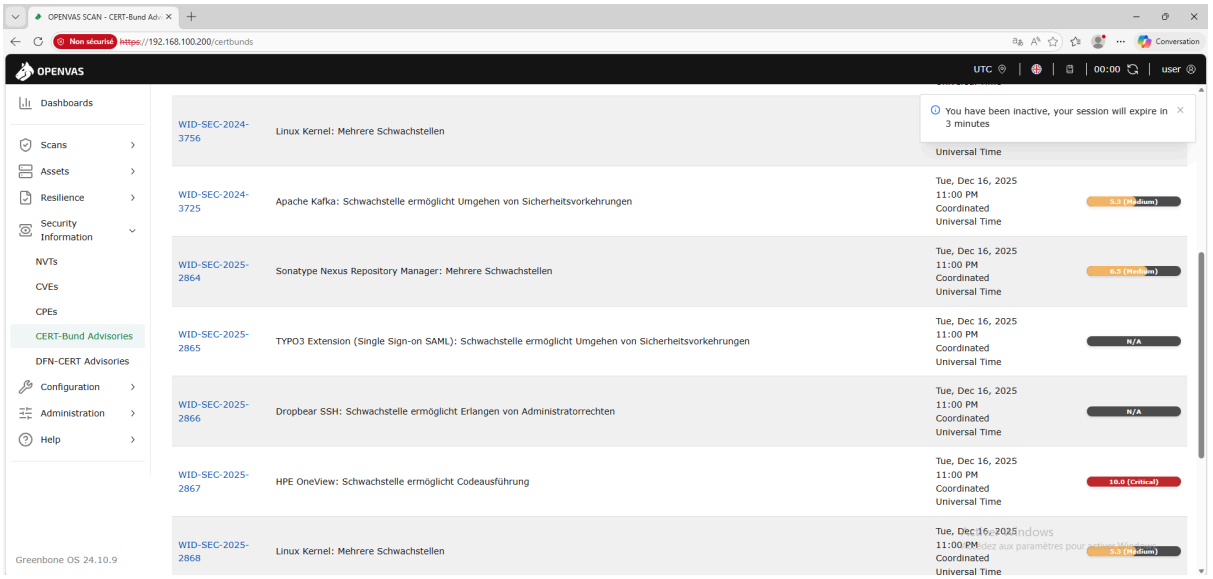
Analyse détaillée des alertes CERT-Bund et des niveaux de sévérité associés aux failles détectées.



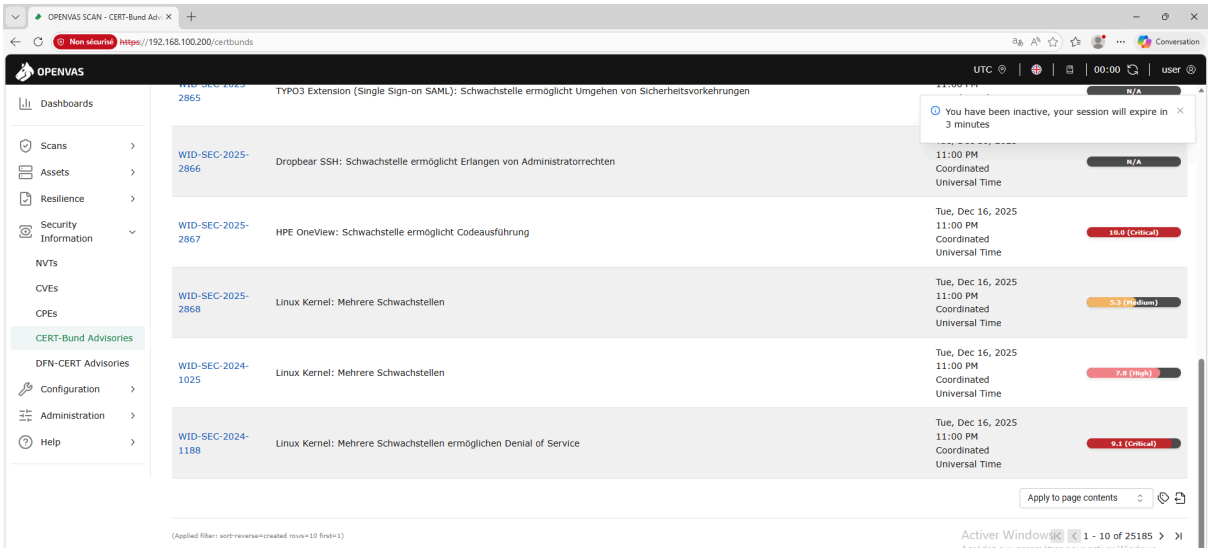
Consultation des avis DFN-CERT concernant les vulnérabilités identifiées lors du scan.



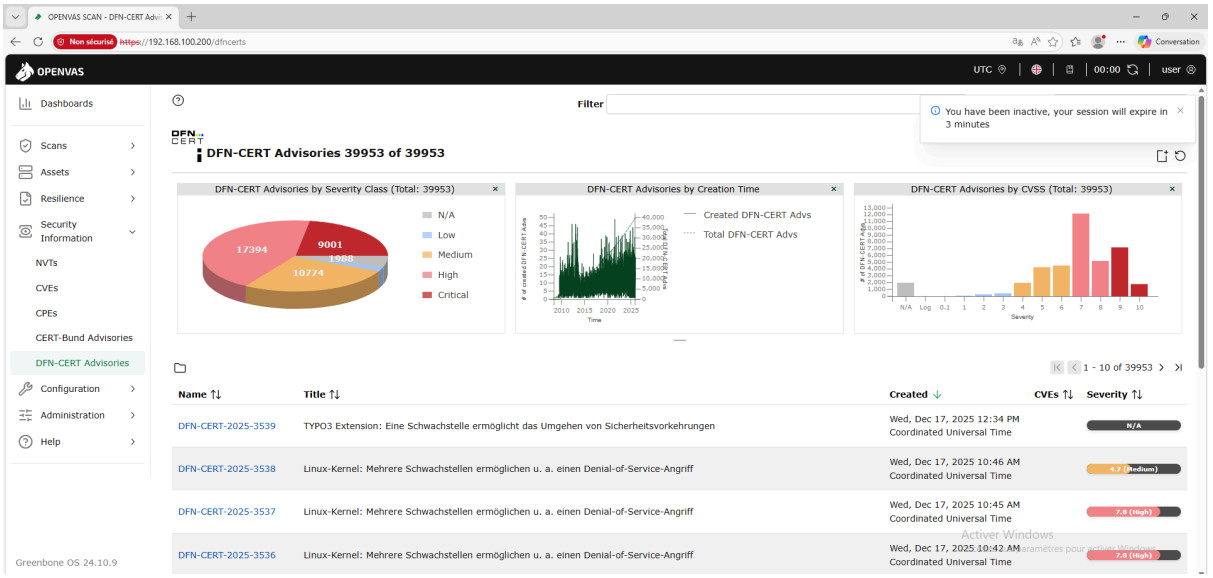
Analyse détaillée des alertes DFN-CERT et des recommandations de sécurité associées.



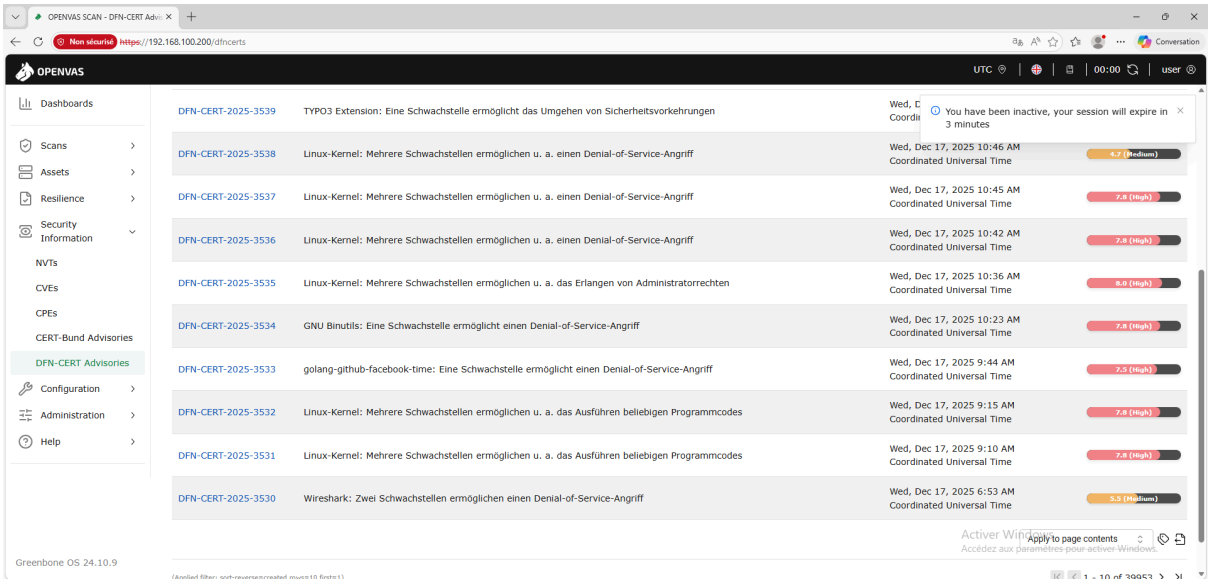
Consultation des politiques de conformité et des modèles d'audit de sécurité disponibles dans OpenVAS.



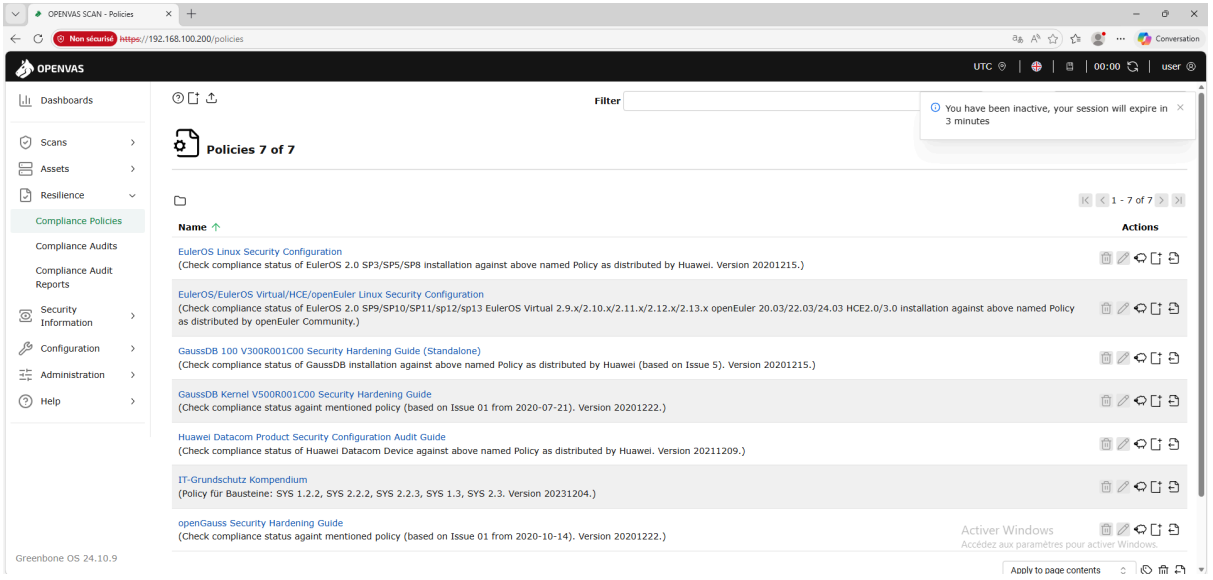
Affichage de la liste des vulnérabilités détectées sur Damn Vulnerable Linux avec leur criticité.



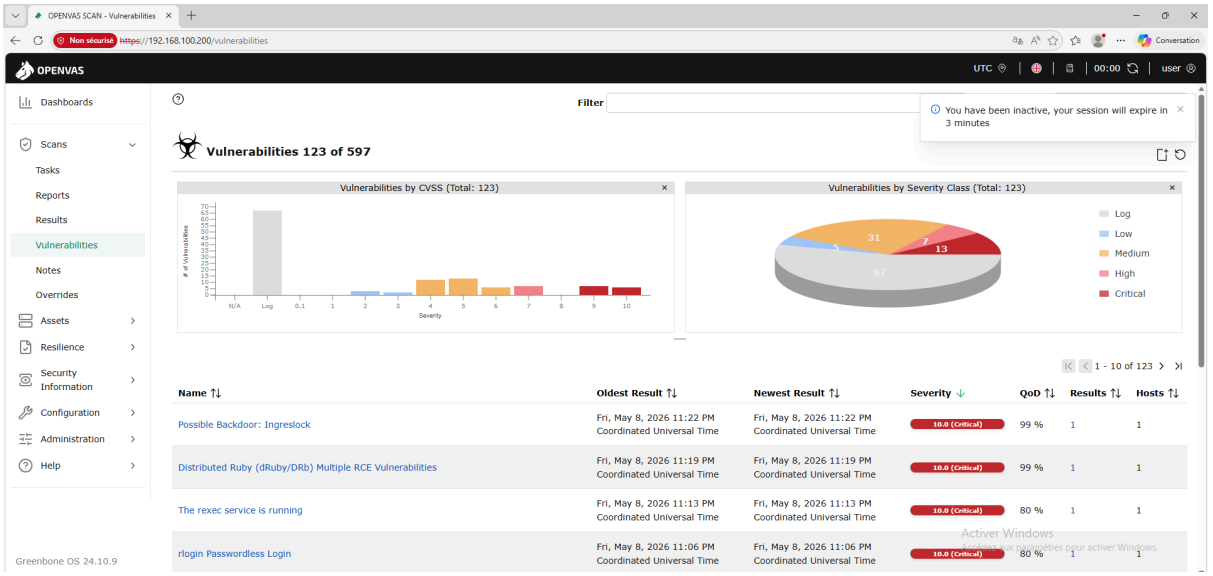
Analyse détaillée des principales failles de sécurité identifiées pendant le scan OpenVAS.



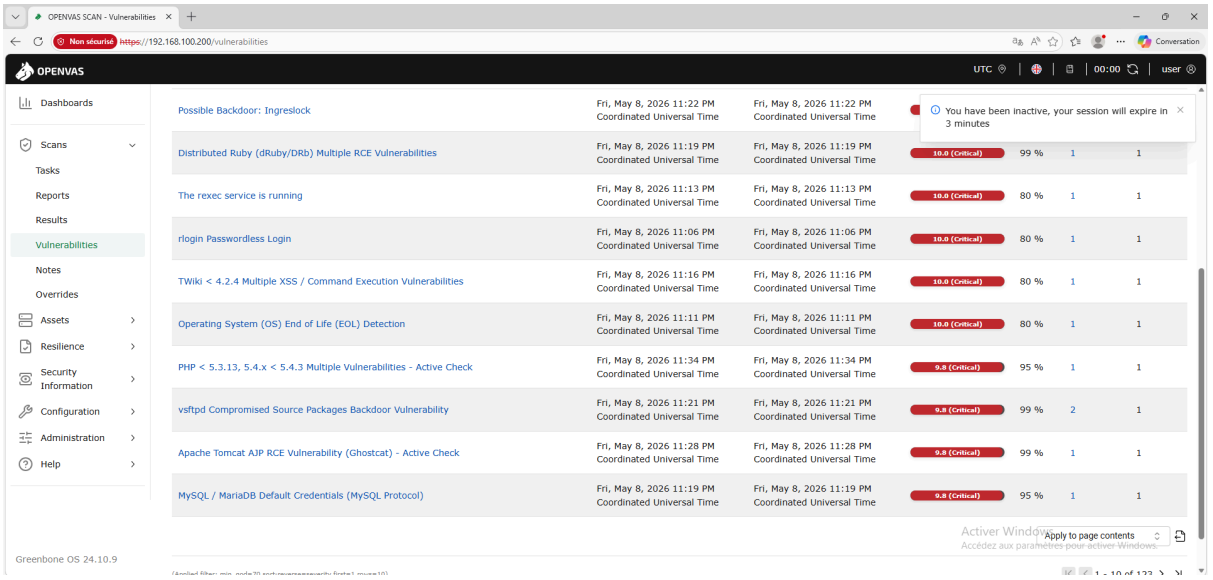
Consultation des politiques de conformité et des modèles d'audit de sécurité disponibles dans OpenVAS.



Affichage de la liste des vulnérabilités détectées sur Damn Vulnerable Linux avec leur niveau de sévérité.



Analyse détaillée des failles de sécurité critiques identifiées pendant le scan OpenVAS.



6. Travail à faire

6.1 Recherches de vulnérabilités

a) Scans > Tasks

Deux tâches de scan ont été créées dans ce TP afin d'analyser les machines Metasploitable et Damn Vulnerable Linux.

Fonctionnalité : Le menu **Tasks** permet de créer et gérer des tâches de scan de vulnérabilités sur différentes machines du réseau. Dans le compte rendu, deux tâches ont été créées : une pour la VM Metasploitable et une autre pour Damn Vulnerable Linux avec le profil Full and fast.

Notions associées :

- Scan de vulnérabilités
- Profil de scan "Full and fast"
- Machine cible
- Planification et suivi des scans
- Analyse réseau

Utilisation professionnelle : Dans une entreprise, ce menu est utilisé pour automatiser les audits de sécurité sur les serveurs, postes clients ou équipements réseau afin de vérifier régulièrement leur niveau de sécurité.

Apport à la sécurité : Cette fonctionnalité permet d'identifier rapidement les systèmes vulnérables présents sur le réseau et de surveiller l'évolution des risques de sécurité.

b) Scans > Reports

Les rapports générés permettent d'avoir une vue globale des vulnérabilités détectées après le scan.

Fonctionnalité : Le menu **Reports** permet de consulter les rapports générés après les scans de sécurité. Les rapports affichent le score de sévérité, le nombre de vulnérabilités détectées, les ports ouverts et les informations techniques du scan.

Notions associées :

- Rapport de scan
- Score CVSS
- Criticité des vulnérabilités
- Historique des analyses

Utilisation professionnelle : Dans une entreprise, ces rapports servent à suivre les vulnérabilités détectées sur les serveurs et postes clients.

Apport à la sécurité : Les rapports permettent de prioriser les vulnérabilités critiques afin de réduire les risques d'attaque sur l'infrastructure.

c) Scans > Results

Fonctionnalité : Le menu **Results** affiche le détail des résultats détectés pendant les scans OpenVAS, notamment les failles de sécurité, les ports ouverts et les services vulnérables.

Notions associées :

- Résultats de scan
- Services réseau
- Détection de vulnérabilités
- Analyse des risques

Utilisation professionnelle : Cette vue permet d'analyser plus précisément les vulnérabilités détectées sur chaque machine analysée.

Apport à la sécurité : Cette fonctionnalité facilite l'identification des services exposés et des vulnérabilités critiques présentes sur les machines du réseau.

d) Scans > Vulnerabilities

Plusieurs vulnérabilités critiques ont été détectées pendant les analyses réalisées avec OpenVAS. Certaines vulnérabilités détectées possédaient un score CVSS élevé avec un niveau de criticité critique.

Fonctionnalité : Le menu **Vulnerabilities** regroupe l'ensemble des vulnérabilités détectées par OpenVAS avec leur niveau de criticité et leur score de sévérité. Plusieurs vulnérabilités critiques ont été détectées sur les machines Metasploitable et Damn Vulnerable Linux.

Notions associées :

- CVE
- CVSS
- Failles critiques
- Sévérité des vulnérabilités

Utilisation professionnelle : Les administrateurs réseau et sécurité utilisent cette vue pour suivre les failles présentes sur les équipements et organiser les actions de remédiation.

Apport à la sécurité : Cela permet de repérer rapidement les vulnérabilités les plus critiques afin de limiter les risques d'attaque.

6.2 Gestion des actifs

e) Assets > Hosts

Fonctionnalité : Le menu **Hosts** affiche les machines détectées pendant les scans avec leur adresse IP et leur niveau de criticité. Les hôtes Metasploitable et Damn Vulnerable Linux ont été identifiés automatiquement pendant les analyses.

Notions associées :

- Inventaire réseau
- Adresse IP
- Hôtes détectés
- Cartographie réseau

Utilisation professionnelle : Ce menu permet de maintenir un inventaire des équipements présents sur le réseau de l'entreprise.

Apport à la sécurité : Cette fonctionnalité aide à repérer les équipements vulnérables ou inconnus présents sur le réseau interne.

f) Assets > Operating Systems

Fonctionnalité : Le menu **Operating Systems** permet d'identifier automatiquement les systèmes d'exploitation détectés pendant les scans OpenVAS.

Notions associées :

- Fingerprinting
- Détection système
- Linux
- Versions système

Utilisation professionnelle : Ce menu permet d'identifier les systèmes obsolètes ou vulnérables afin de préparer les mises à jour nécessaires.

Apport à la sécurité : Cette fonctionnalité permet de détecter les systèmes non sécurisés ou non mis à jour présents dans l'infrastructure.

g) Assets > TLS Certificates

Fonctionnalité : Le menu **TLS Certificates** permet d'afficher les certificats TLS détectés pendant les scans de sécurité OpenVAS.

Notions associées :

- Certificats TLS/SSL
- HTTPS
- Chiffrement
- Sécurité des communications

Utilisation professionnelle : Les administrateurs utilisent cette vue pour vérifier la validité des certificats utilisés sur les serveurs de l'entreprise.

Apport à la sécurité : Ce menu permet d'identifier les certificats expirés ou mal configurés qui peuvent rendre les communications moins sécurisées.

6.3 Resilience

h) Resilience > Compliance Policies

Fonctionnalité : Le menu **Compliance Policies** permet de consulter les politiques de conformité et les modèles d'audit de sécurité disponibles dans OpenVAS.

Notions associées :

- Politique de conformité
- Audit de sécurité

- Bonnes pratiques
- Configuration sécurisée

Utilisation professionnelle : Ces politiques sont utilisées lors des audits de sécurité pour vérifier la conformité des systèmes.

Apport à la sécurité : Cela permet de mieux sécuriser les machines du réseau et de repérer les configurations vulnérables.

6.4 Security Information

Fonctionnalité : Le menu **Security Information** permet de consulter les différentes bases de vulnérabilités utilisées par Greenbone comme les NVT, CVE, CERT et CPE.

Notions associées :

- NVT (Network Vulnerability Test)
- CVE
- CERT
- CPE

Utilisation professionnelle : Ces informations permettent de mieux comprendre les vulnérabilités détectées par OpenVAS et les risques associés aux machines analysées.

Apport à la sécurité : Cette fonctionnalité permet d'obtenir des informations détaillées sur les failles de sécurité et leurs impacts potentiels.

6.5 Gestion des cibles

i) Configuration > Targets

Les adresses IP des machines vulnérables ont été configurées manuellement dans les cibles OpenVAS.

Fonctionnalité : Le menu **Targets** permet de définir les machines ou réseaux qui seront analysés par les scans OpenVAS. Les cibles Metasploitable et Damn Vulnerable Linux ont été configurées pour les tests de vulnérabilités.

Notions associées :

- Adresse IP cible
- Réseau cible
- Configuration de scan
- Scope de sécurité

Utilisation professionnelle : Les équipes de sécurité peuvent utiliser cette fonctionnalité afin de surveiller les machines présentes sur le réseau.

Apport à la sécurité : Cette fonctionnalité permet de contrôler précisément les systèmes surveillés et d'éviter les oublis pendant les audits de sécurité.

6.6 Définition des identifiants

j) Configuration > Credentials

Aucun identifiant SSH ou SMB n'a été configuré pendant ce TP.

Fonctionnalité : Le menu **Credentials** permet d'ajouter des identifiants SSH, SMB ou autres afin de réaliser des scans authentifiés plus complets. Dans ce TP, aucun identifiant n'a été configuré.

Notions associées :

- Scan authentifié
- SSH
- SMB
- Authentification système

Utilisation professionnelle : Les scans authentifiés permettent d'obtenir des résultats plus précis sur les systèmes analysés.

Apport à la sécurité : Cette fonctionnalité améliore la détection des vulnérabilités locales et des mauvaises configurations système.