

BTS 2 - Services Informatiques aux Organisations

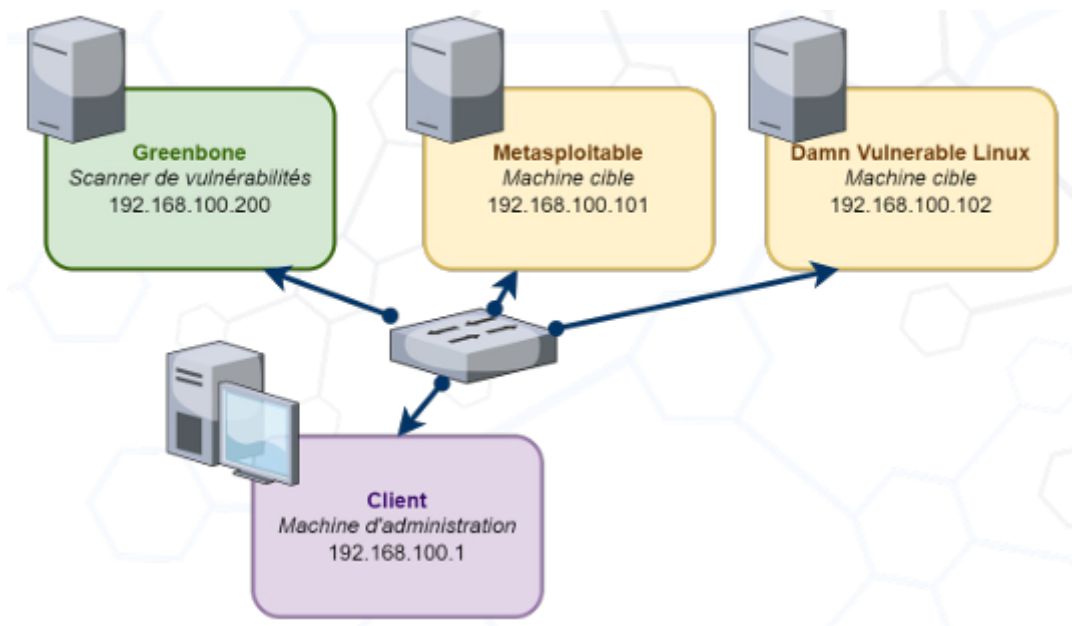


BTS SIO SISR – Recherche de vulnérabilité : Greenbone

Tables des matières :

Topologie réseau.....	3
1. Installation et configuration de Metasploitable.....	4
2. Installation et configuration de Damn Vulnerable Linux.....	5
3. Installation et configuration de Greenbone.....	8
3.1 Configuration de la machine virtuelle.....	8
3.2 Première configuration à l'aide de l'assistant.....	10
3.3 Description des menus.....	13
a) Menu général d'administration.....	13
b) Menu Administration > Setup.....	14
c) Menu Administration > Maintenance.....	15
d) Menu Administration > About.....	15
3.4 Configuration du réseau.....	16
3.5 Connexion interface Web.....	20
3.6 Mise à jour des listes de définition de vulnérabilité.....	21
e) Configuration du serveur de mise à jour.....	22
f) Mise à jour.....	24
4. Test avec la VM Metasploitable.....	26
5. Test avec la VM Damn Vulnerable Linux.....	46
6. Travail à faire.....	63
6.1 Recherches de vulnérabilités.....	63
a) Scans > Tasks.....	63
b) Scans > Reports.....	63
c) Scans > Results.....	64
d) Scans > Vulnerabilities.....	64
6.2 Gestion des actifs.....	65
e) Assets > Hosts.....	65
f) Assets > Operating Systems.....	65
g) Assets > TLS Certificates.....	66
6.3 Resilience.....	66
h) Resilience > Compliance Policies.....	66
6.4 Security Information.....	67
6.5 Gestion des cibles.....	67
i) Configuration > Targets.....	67
6.6 Définition des identifiants.....	68
j) Configuration > Credentials.....	68

Topologie réseau

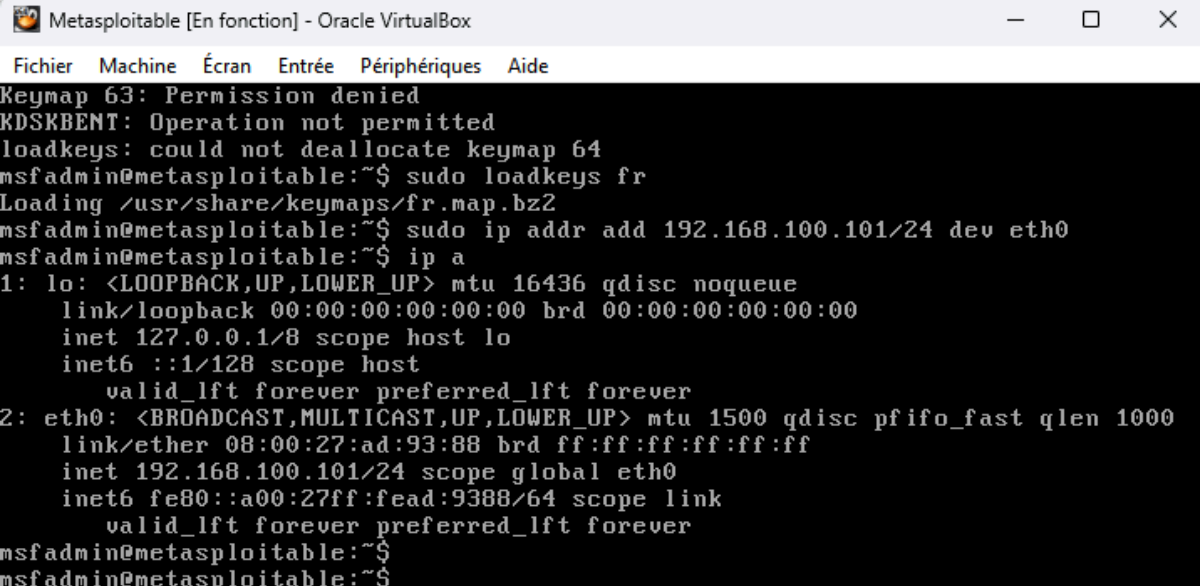


Configuration Réseau

	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

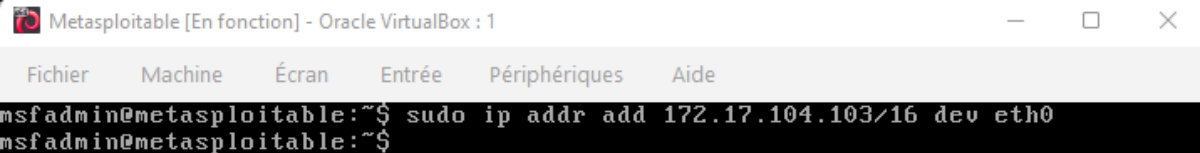
1. Installation et configuration de Metasploitable

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



```
Metasploitable [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Keymap 63: Permission denied
KDSKBENT: Operation not permitted
loadkeys: could not deallocate keymap 64
msfadmin@metasploitable:~$ sudo loadkeys fr
Loading /usr/share/keymaps/fr.map.bz2
msfadmin@metasploitable:~$ sudo ip addr add 192.168.100.101/24 dev eth0
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:ad:93:88 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.101/24 scope global eth0
    inet6 fe80::a00:27ff:fead:9388/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

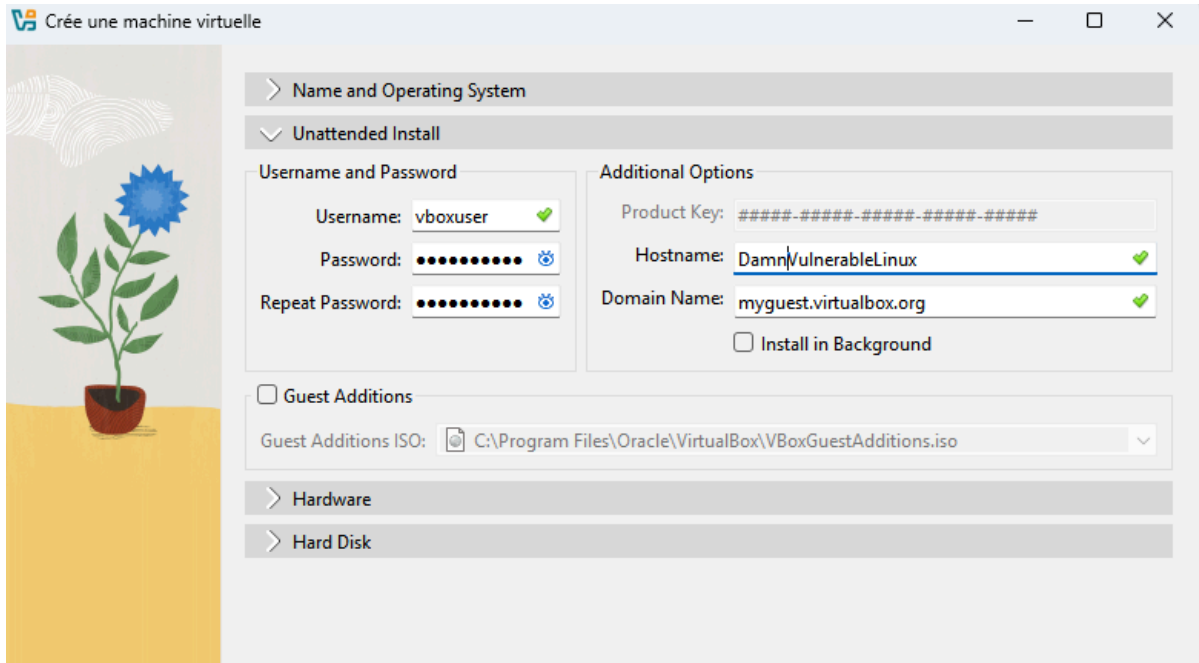
Configuration de l'adresse IP de la machine cible Metasploitable pour permettre le scan réseau avec Greenbone.



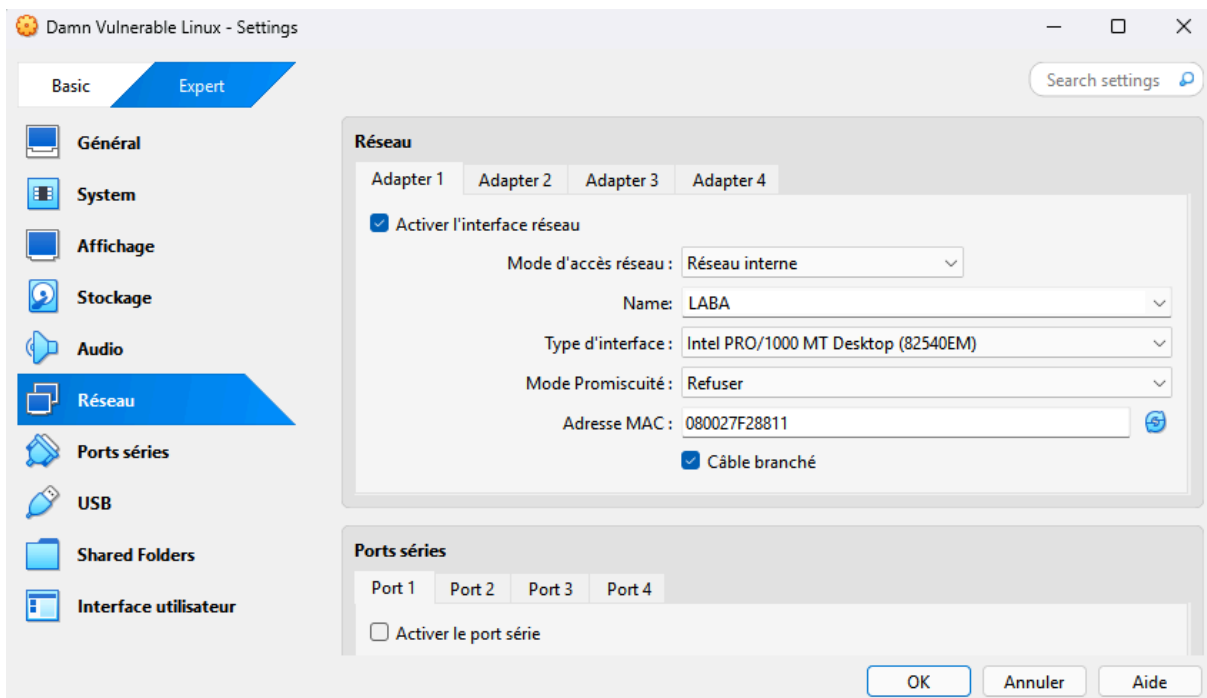
```
Metasploitable [En fonction] - Oracle VirtualBox : 1
Fichier Machine Écran Entrée Périphériques Aide
msfadmin@metasploitable:~$ sudo ip addr add 172.17.104.103/16 dev eth0
msfadmin@metasploitable:~$
```

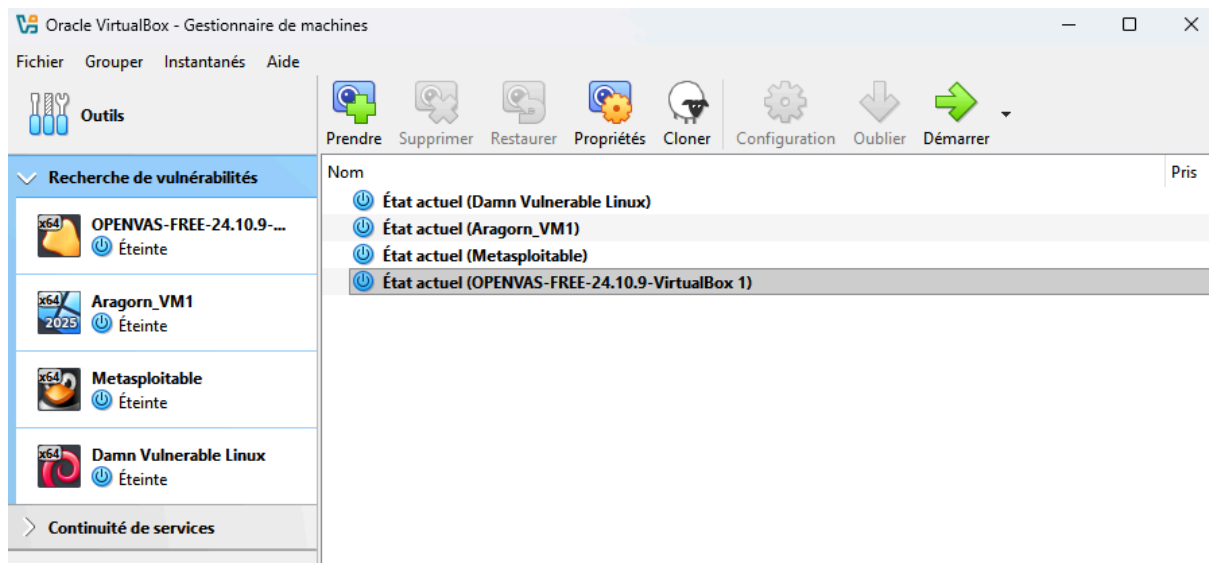
2. Installation et configuration de Damn Vulnerable Linux

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

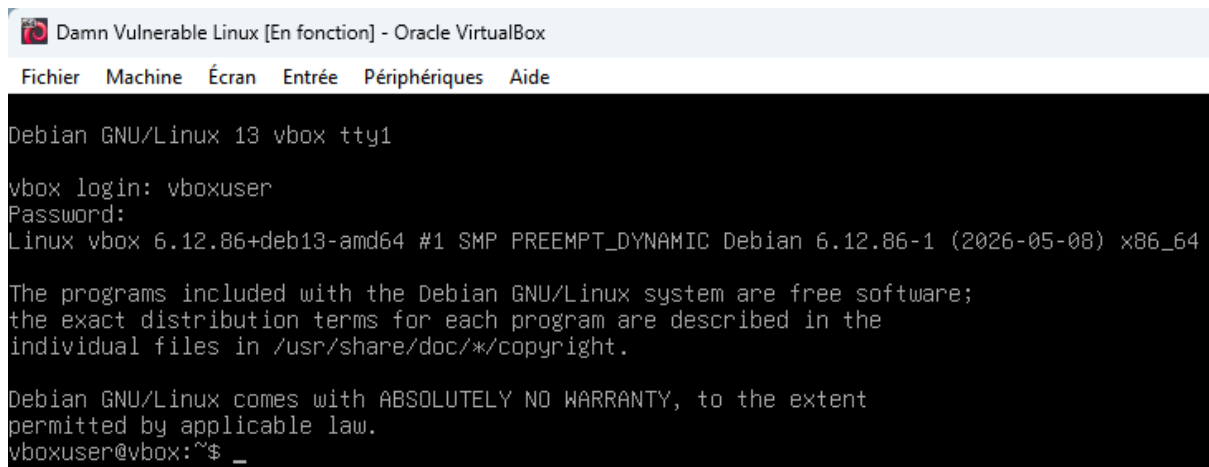


Configuration du réseau interne LABA dans VirtualBox pour isoler les machines du TP.





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.

```
Damn Vulnerable Linux [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 8.4 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#allow-hotplug enp0s3
#iface enp0s3 inet dhcp
auto enp0s3
iface enp0s3 inet static
    address 192.168.100.100
    netmask 255.255.255.0

# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
```

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

```
Damn Vulnerable Linux [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
Debian GNU/Linux 13 vbox tty1
vbox login: vboxuser
Password:
Linux vbox 6.12.86+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.86-1 (2026-05-08) x86_64

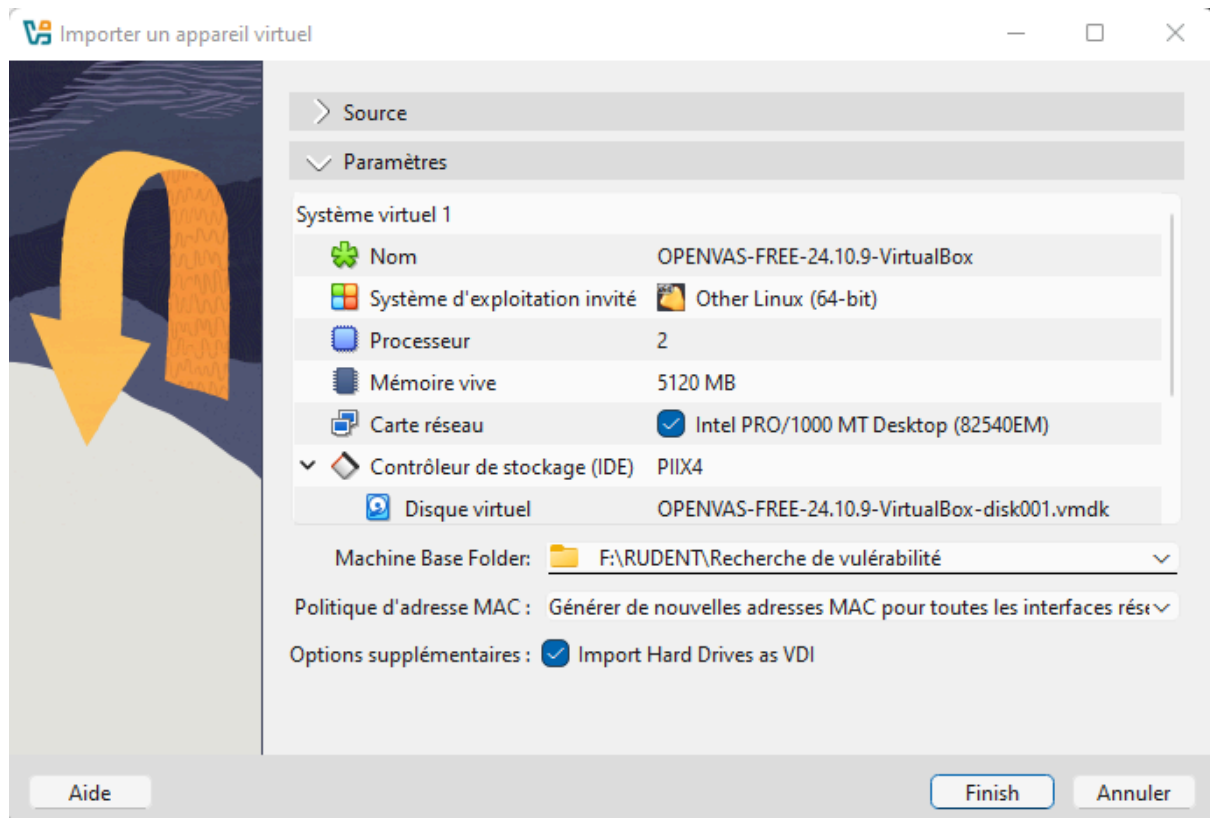
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vboxuser@vbox:~$
vboxuser@vbox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f2:88:11 brd ff:ff:ff:ff:ff:ff
    altname enx080027f28811
    inet 192.168.100.100/24 brd 192.168.100.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef2:8811/64 scope link proto kernel_l1
        valid_lft forever preferred_lft forever
vboxuser@vbox:~$
```

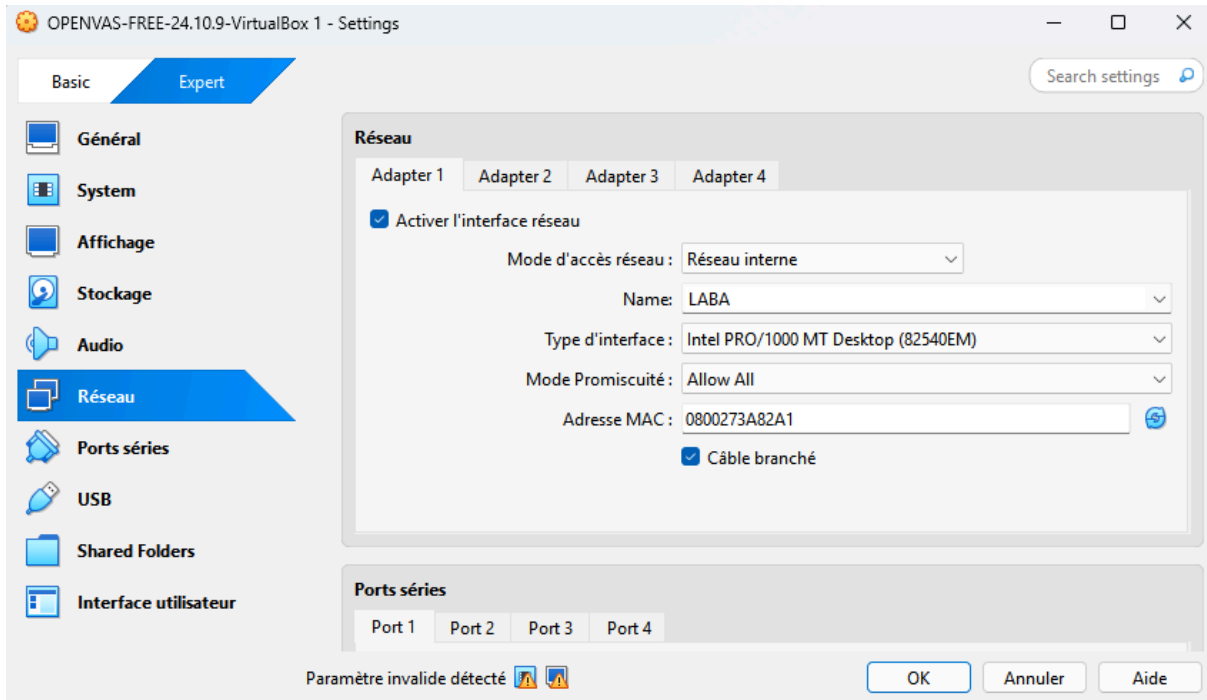
3. Installation et configuration de Greenbone

3.1 Configuration de la machine virtuelle

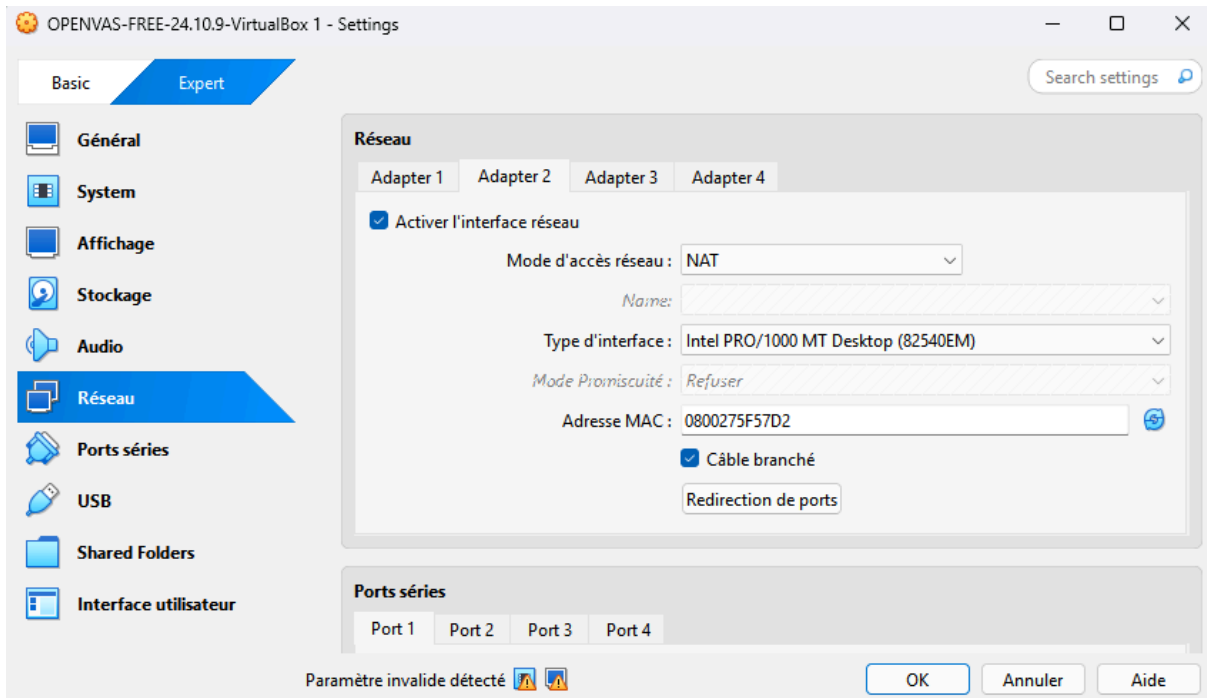
Importation de la machine virtuelle OpenVAS/Greenbone dans VirtualBox afin de préparer l'environnement de scan de vulnérabilités.



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

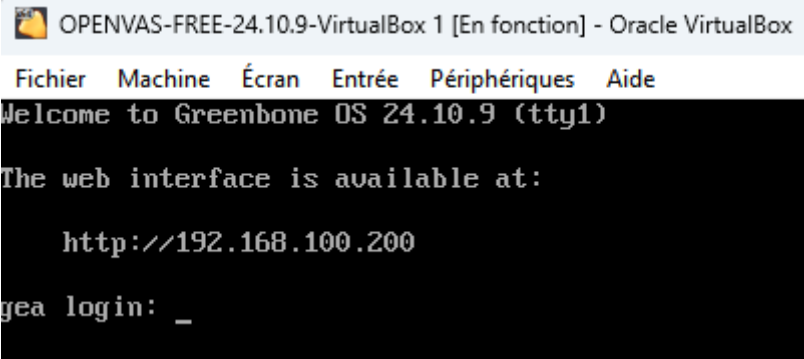


Configuration de l'interface réseau enp0s8 OpenVAS en mode NAT pour permettre l'accès à Internet et les mises à jour de Greenbone.



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.



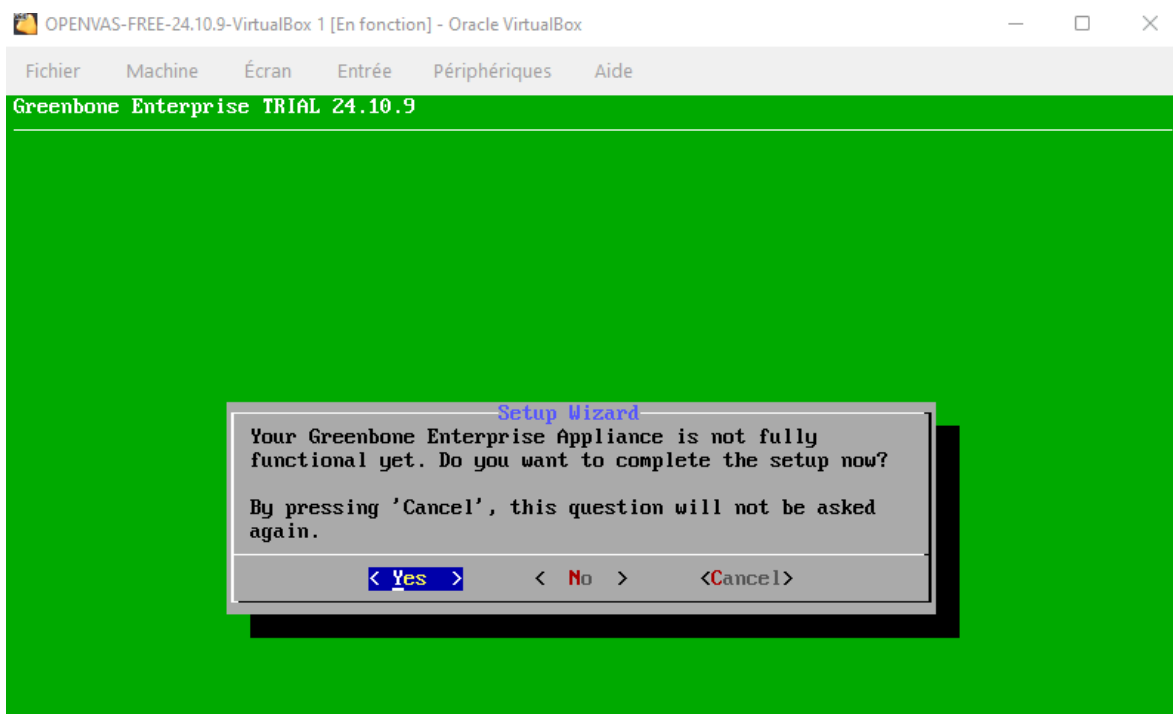
```
OPENVAS-FREE-24.10.9-VirtualBox 1 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
Welcome to Greenbone OS 24.10.9 (tty1)

The web interface is available at:

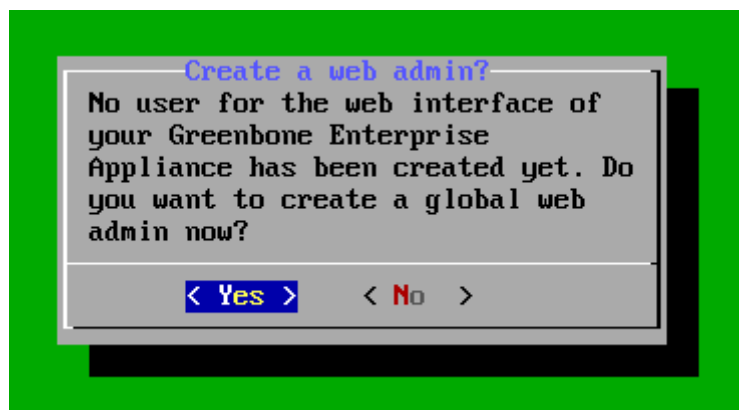
    http://192.168.100.200

gea login: _
```

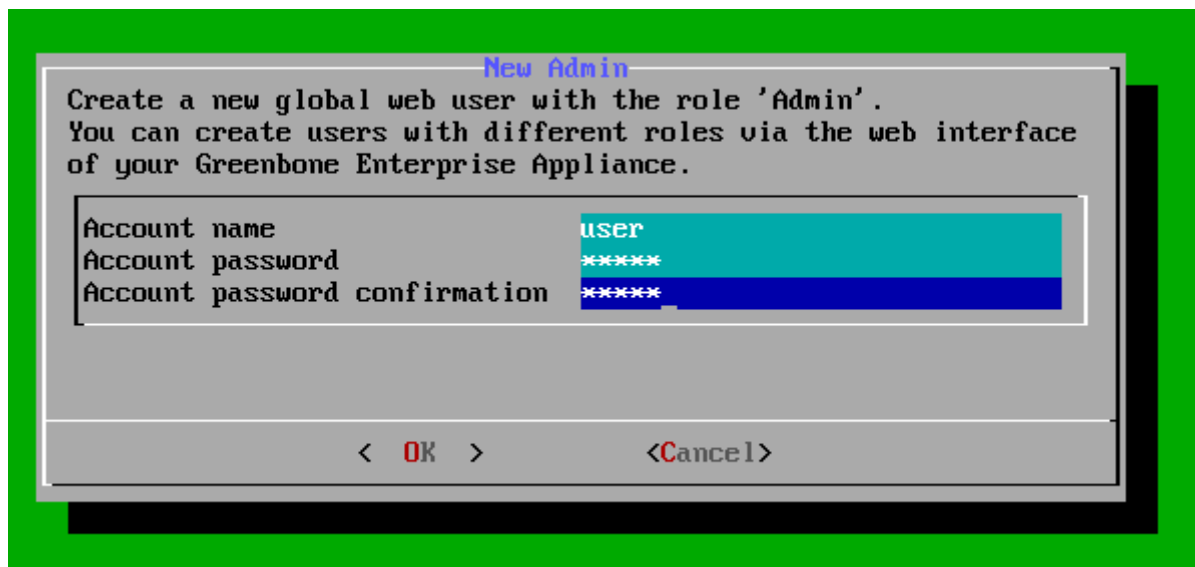
Lancement de l'assistant de configuration initiale de Greenbone afin de finaliser les paramètres du système.



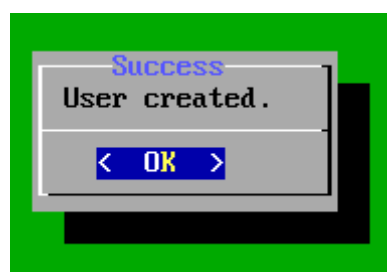
Création du compte administrateur Web pour accéder à l'interface de gestion Greenbone.



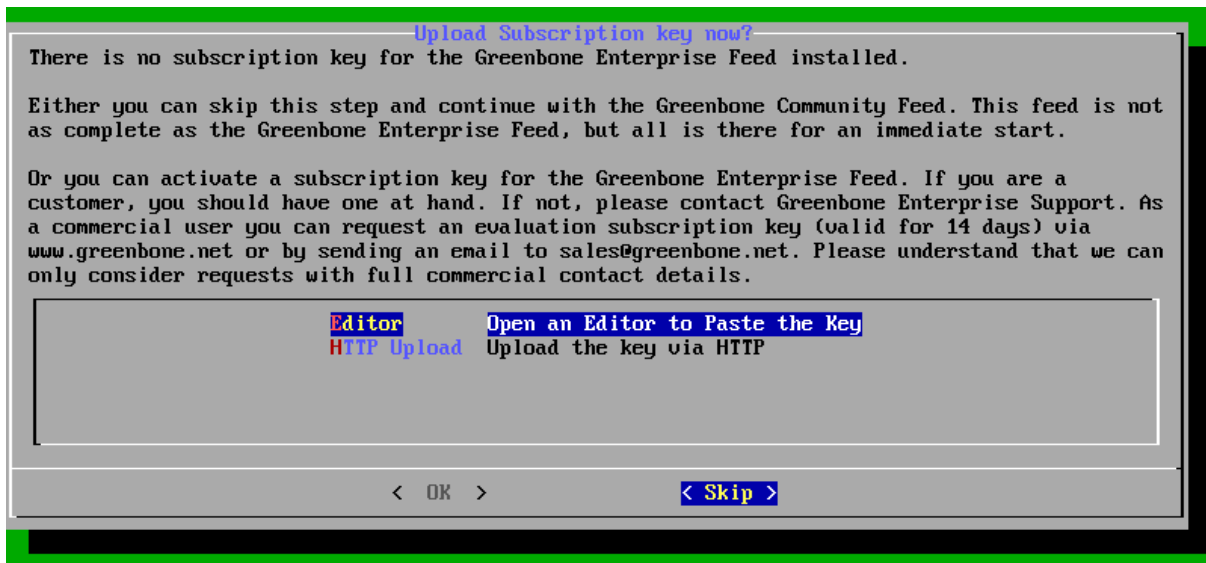
Définition du nom d'utilisateur et du mot de passe du compte administrateur Greenbone.



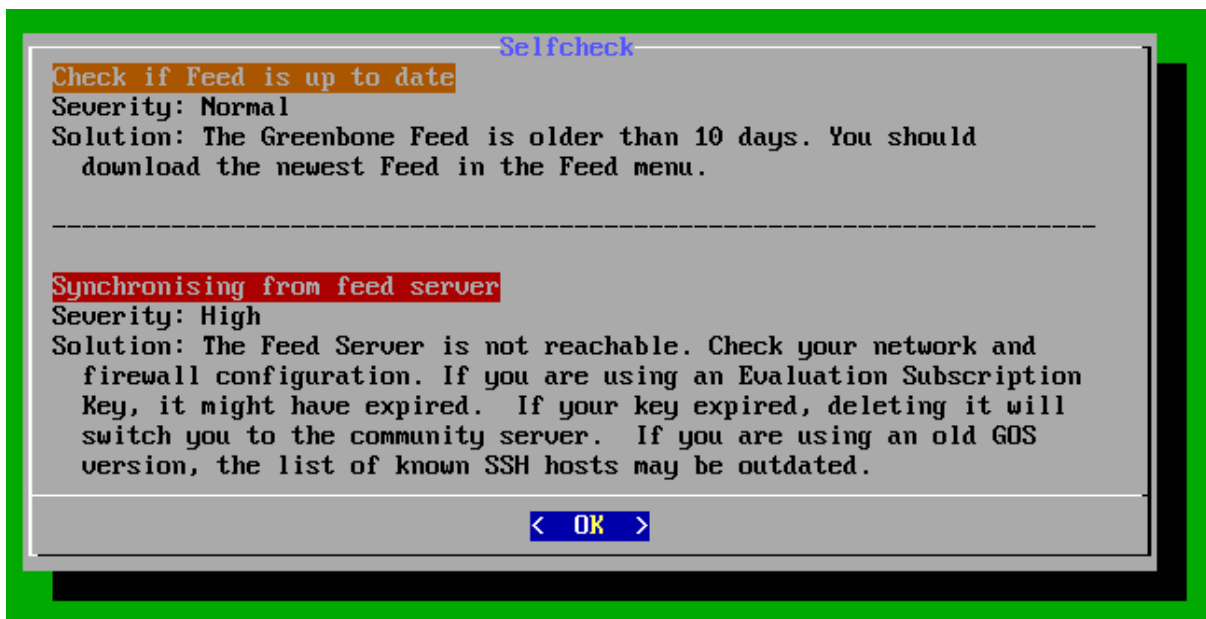
Validation de la création du compte administrateur Greenbone.



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

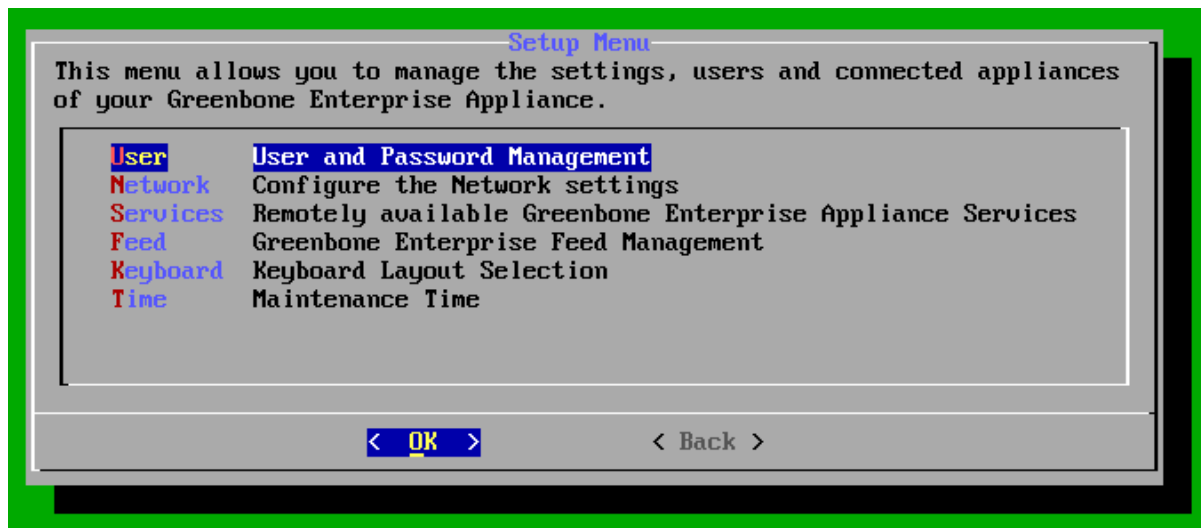
Présentation du menu d'administration principal permettant d'accéder aux fonctions de configuration, maintenance et gestion avancée de Greenbone.



- **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

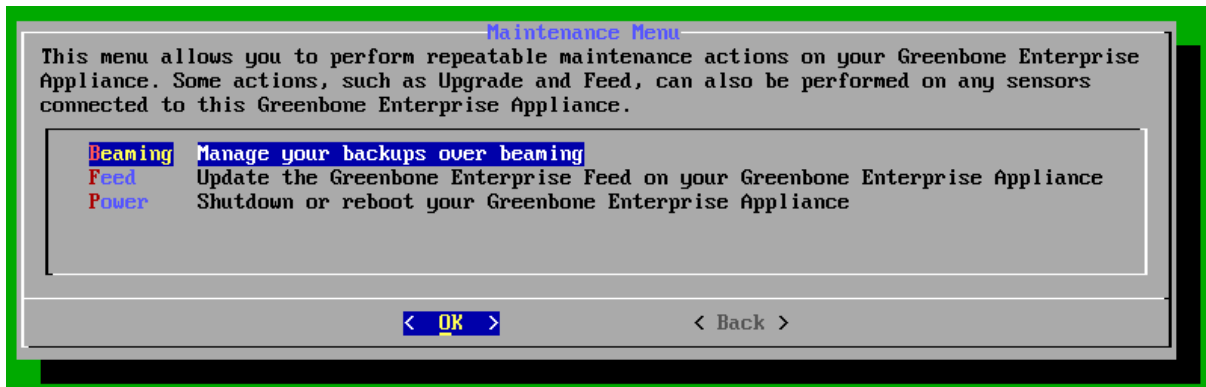
Présentation du menu Setup permettant de gérer les utilisateurs, le réseau, les services et les mises à jour de Greenbone.



- **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

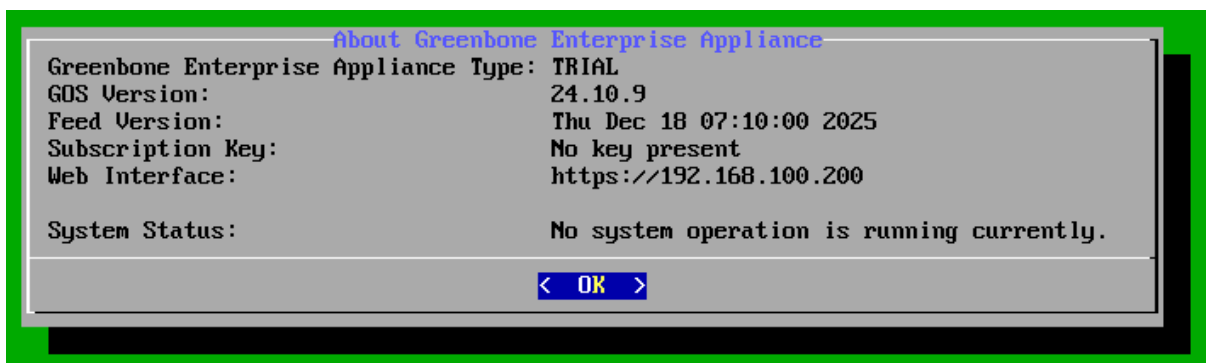
Présentation du menu Maintenance permettant d'effectuer les sauvegardes, les mises à jour et le redémarrage du système Greenbone.



- **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

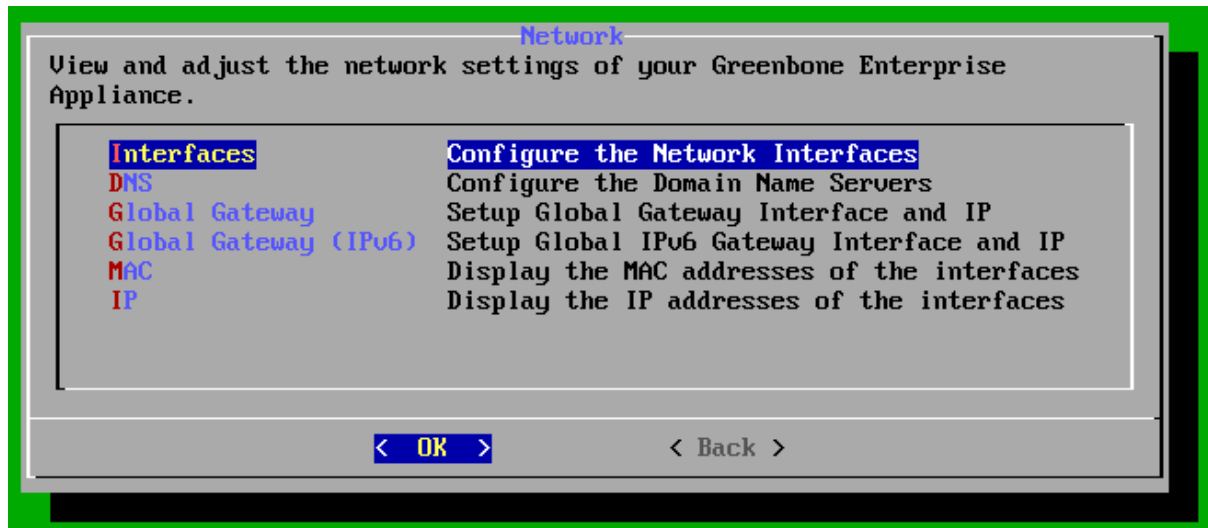
d) Menu Administration > About

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

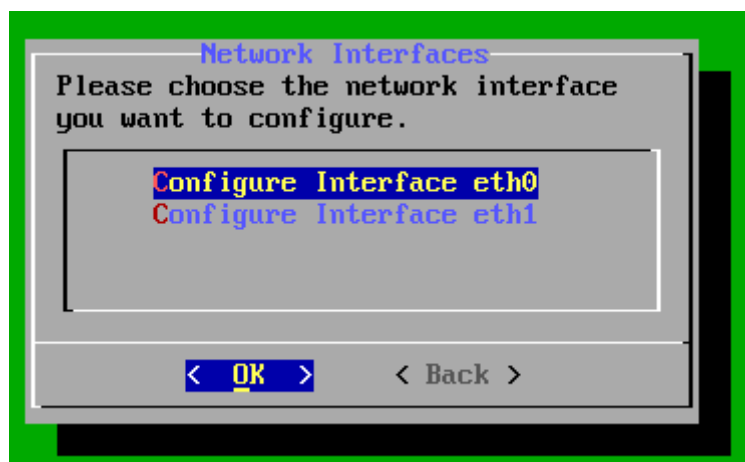


3.4 Configuration du réseau

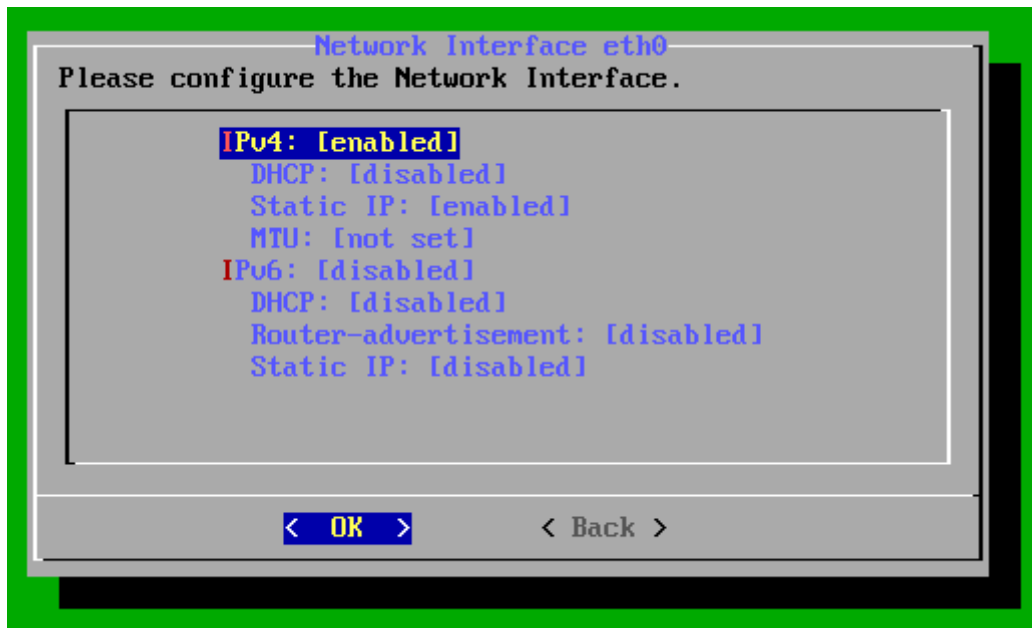
Accès au menu réseau de Greenbone pour configurer les interfaces réseau, les adresses IP et les serveurs DNS.



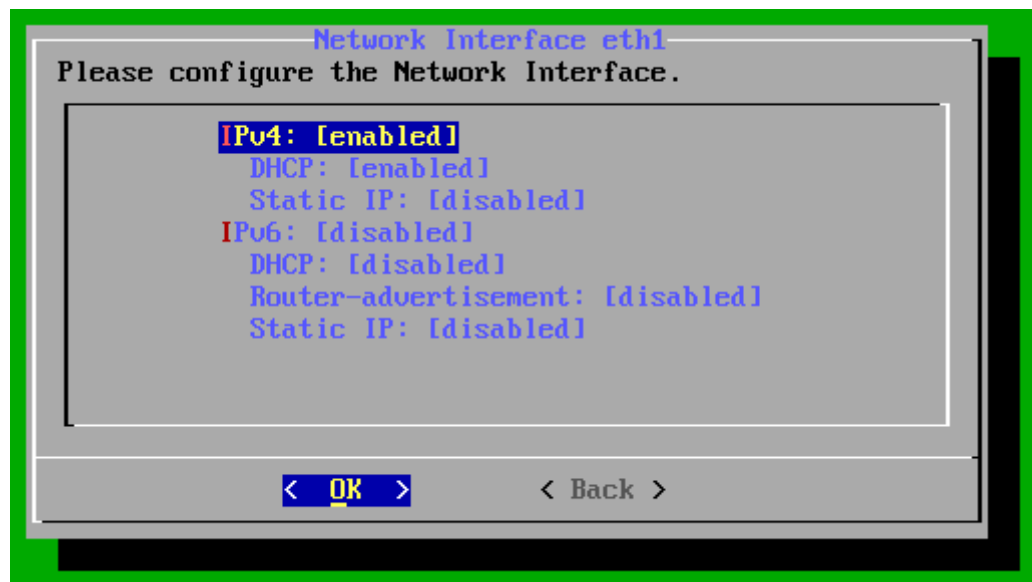
Sélection de l'interface réseau à configurer sur la machine Greenbone.



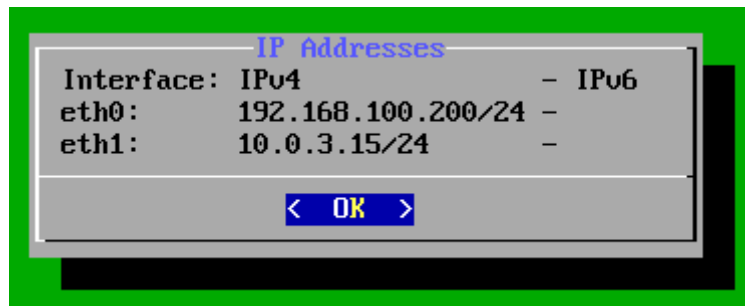
Configuration de l'interface réseau **eth0** avec une adresse IPv4 statique pour le réseau interne du laboratoire.



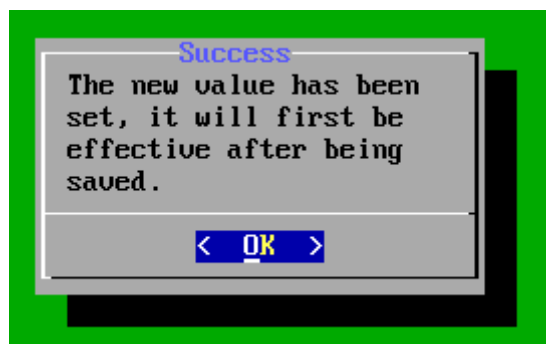
Configuration de l'interface réseau **eth1** en DHCP pour permettre l'accès Internet et les mises à jour Greenbone.



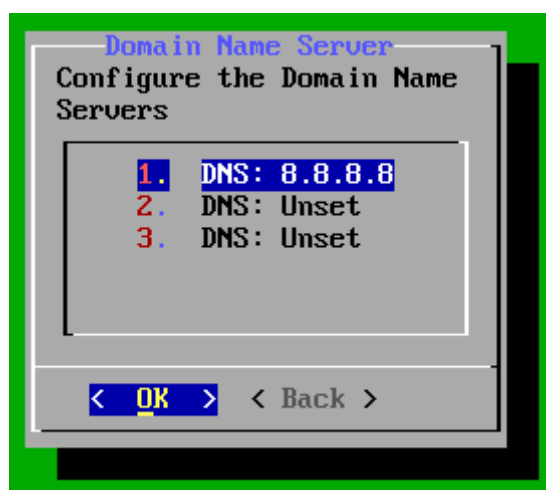
Vérification des adresses IP configurées sur les interfaces réseau de Greenbone.



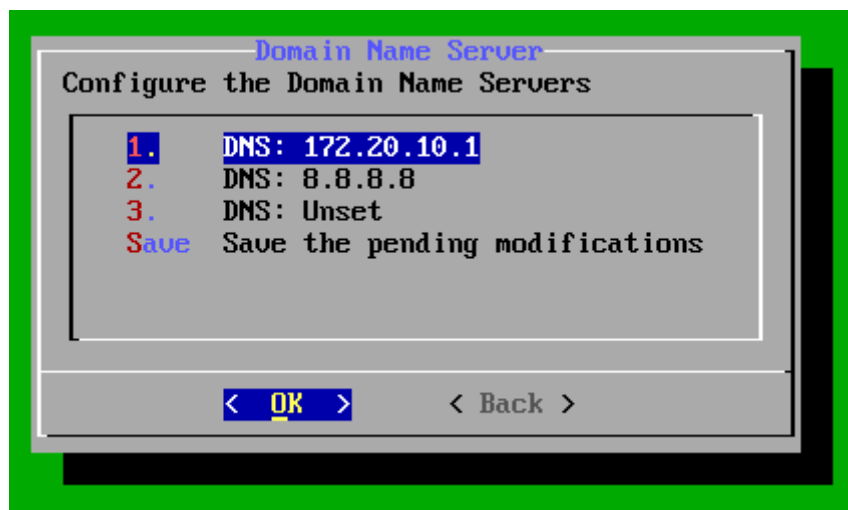
Validation et sauvegarde de la nouvelle configuration réseau du système.



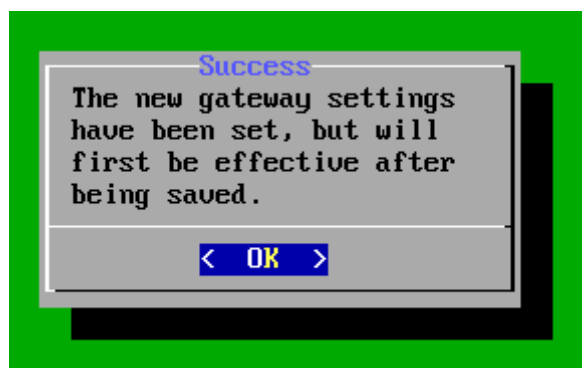
Configuration du serveur DNS Google 8.8.8.8 pour permettre la résolution de noms et les mises à jour Internet.



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

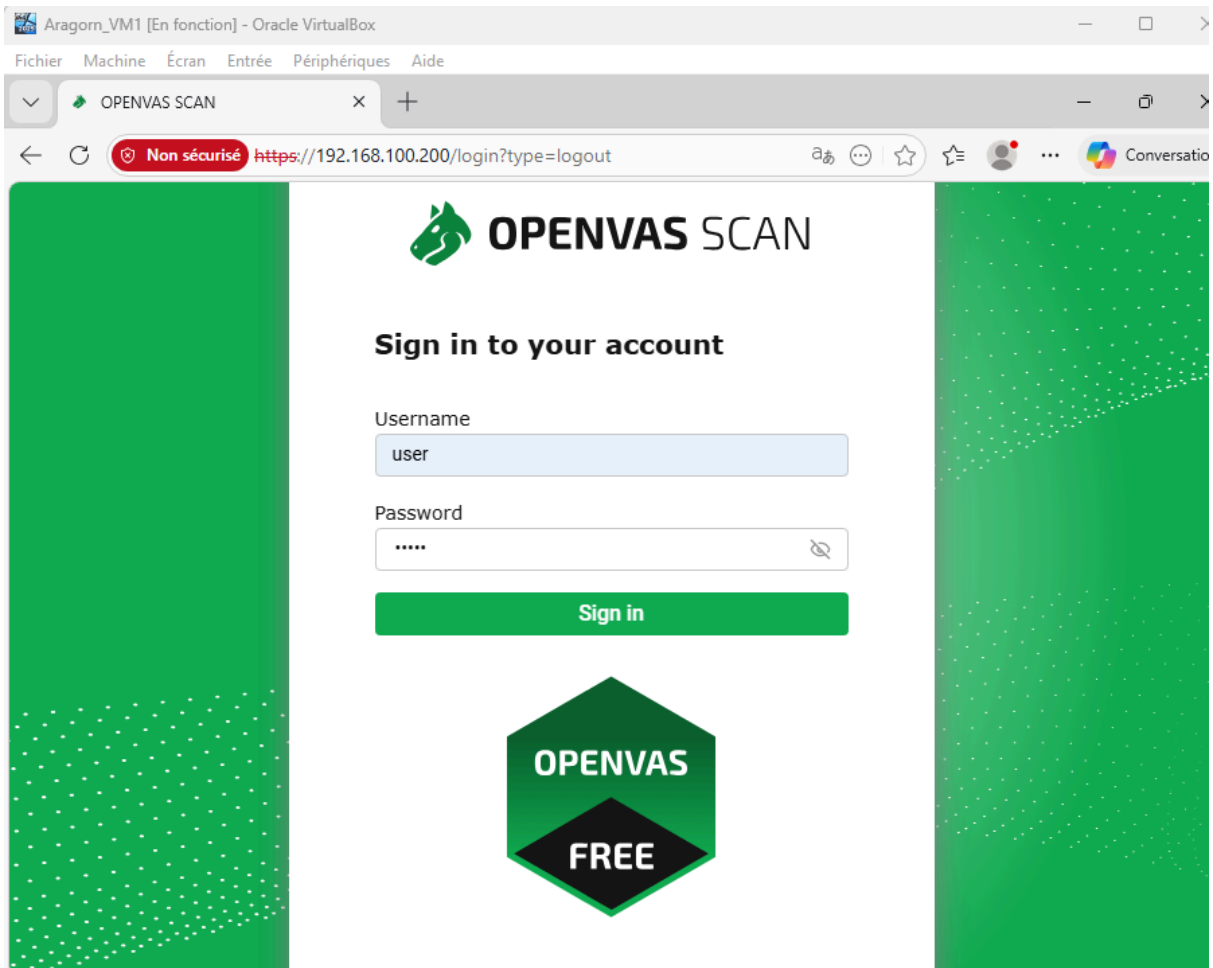


Validation et enregistrement des paramètres DNS configurés sur le système.

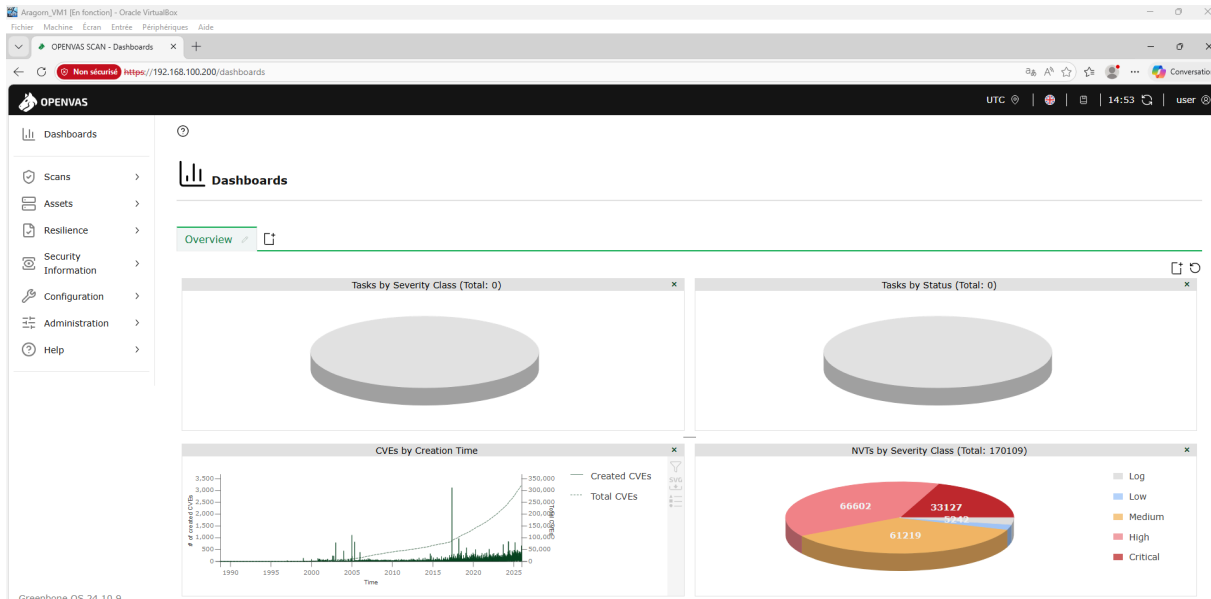


3.5 Connexion interface Web

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.

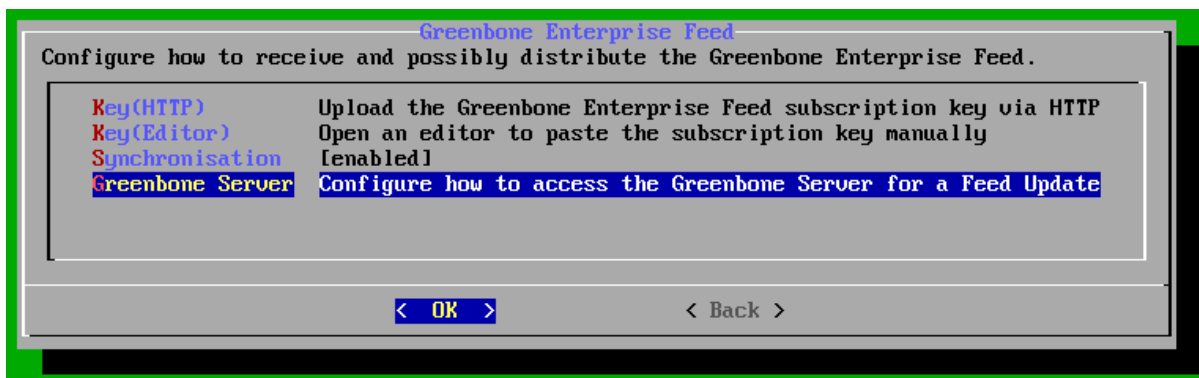
The screenshot shows the 'Feed Status' page in OpenVAS. It displays a table of vulnerability feeds with the following data:

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20251218T0710	Too old (141 days) Please check the automatic synchronization of your system.
SCAP	CVEs, CPEs	Greenbone Community SCAP Feed	20251218T0506	Too old (141 days) Please check the automatic synchronization of your system.
CERT	CERT-Bund Advisories, DFN-CERT Advisories	Greenbone Community CERT Feed	20251218T0420	Too old (141 days) Please check the automatic synchronization of your system.
GVMD_DATA	Compliance Policies, Port Lists, Report Formats, Scan Configs	Greenbone Community gvmd Data Feed	20251218T0507	Too old (141 days) Please check the automatic synchronization of your system.

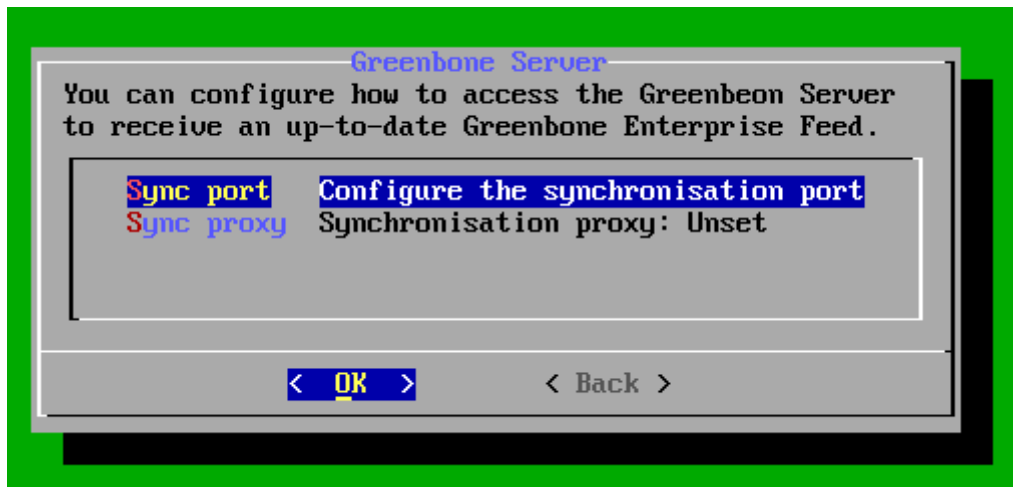
- **NVT (network vulnerability test)** : ce sont des scripts qui sont exécutés sur un systèmes ciblés afin de vérifier la présence de failles. Certains scripts sont génériques et exécutés sur l'ensemble des actifs du réseau, tandis que d'autres ciblent particulièrement un matériel, un logiciel, un service,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

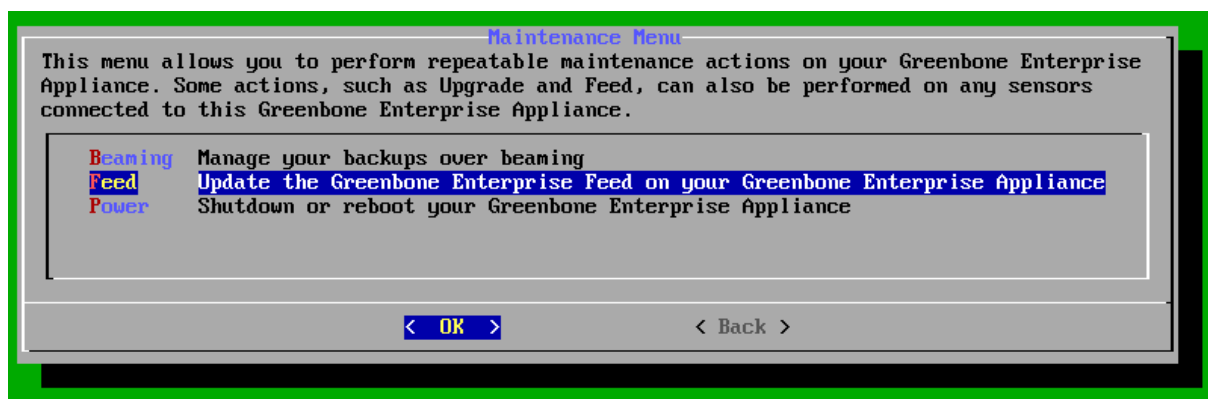


f) Mise à jour

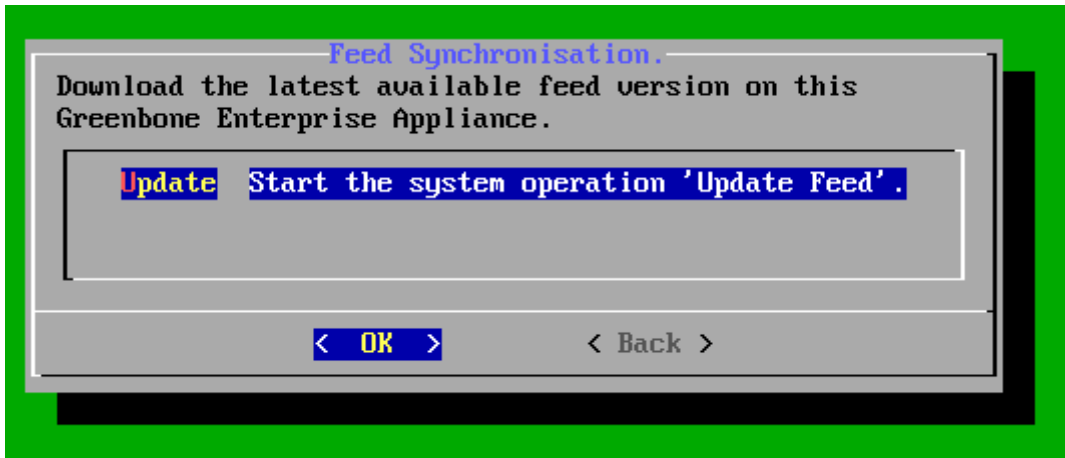
Accès au menu Maintenance afin d'effectuer les opérations de mise à jour et de maintenance de Greenbone.



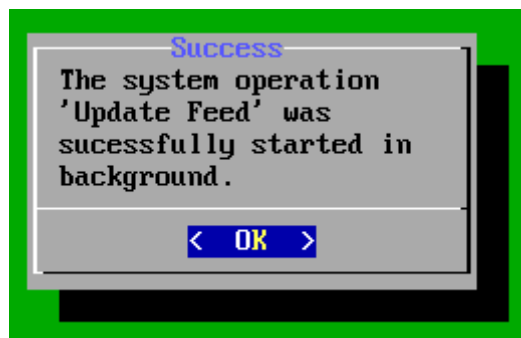
Sélection du menu Feed dans Maintenance pour lancer la mise à jour des bases de vulnérabilités Greenbone.



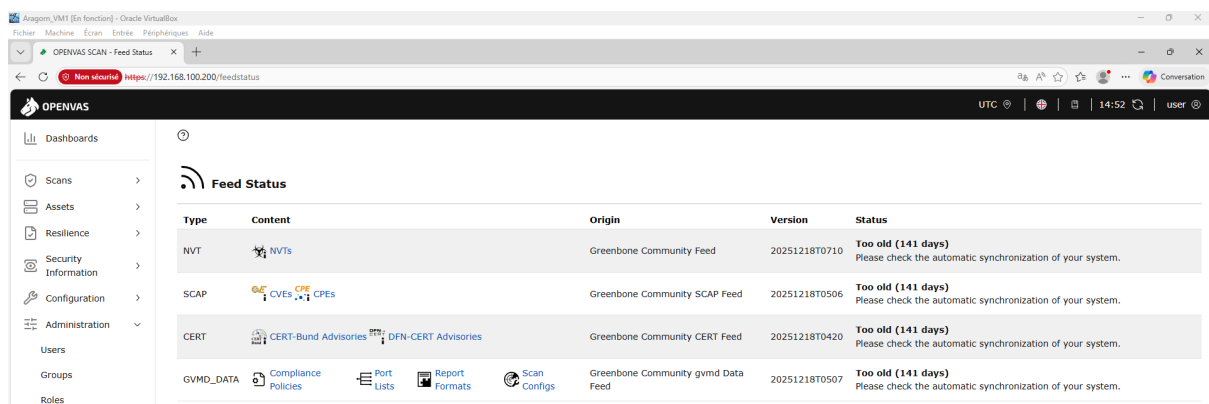
Démarrage de l'opération de synchronisation "Update Feed" afin de télécharger les dernières signatures de vulnérabilités.



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".

Advanced Task Wizard ✕

Quick start: Create a new task

This wizard can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose, whether you want to run the scan immediately or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

For any other setting the defaults from "My Settings" will be applied.

Task Name

Scan Config

Target Host(s)

Start Time
 Start immediately
 Do not start automatically

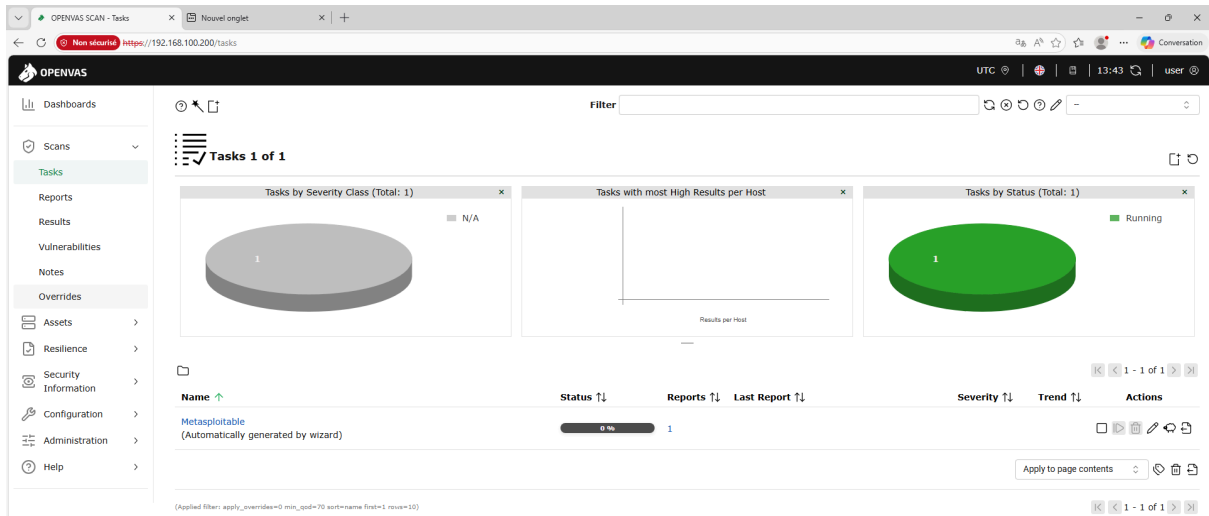
SSH Credential
 on port

SMB Credential

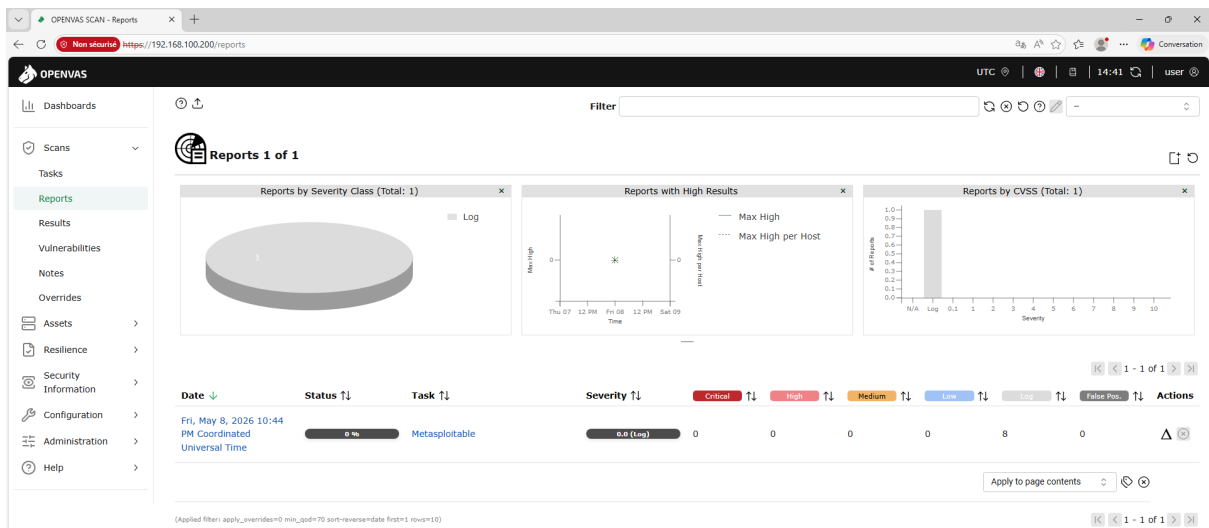
ESXi Credential

Cancel
Create

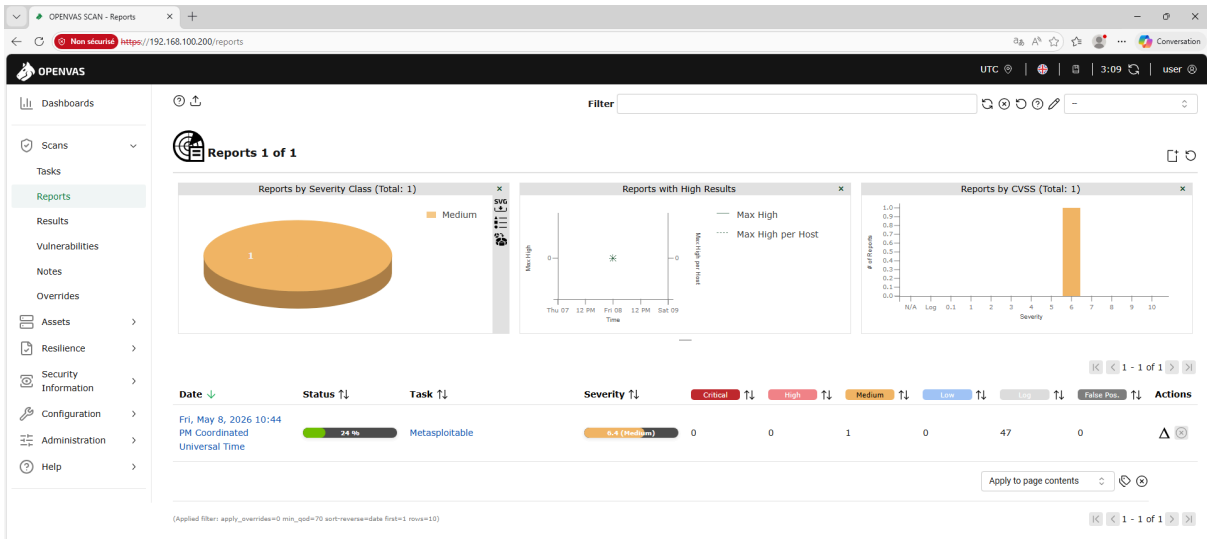
Lancement du scan de vulnérabilités sur la machine Metasploitable depuis OpenVAS.



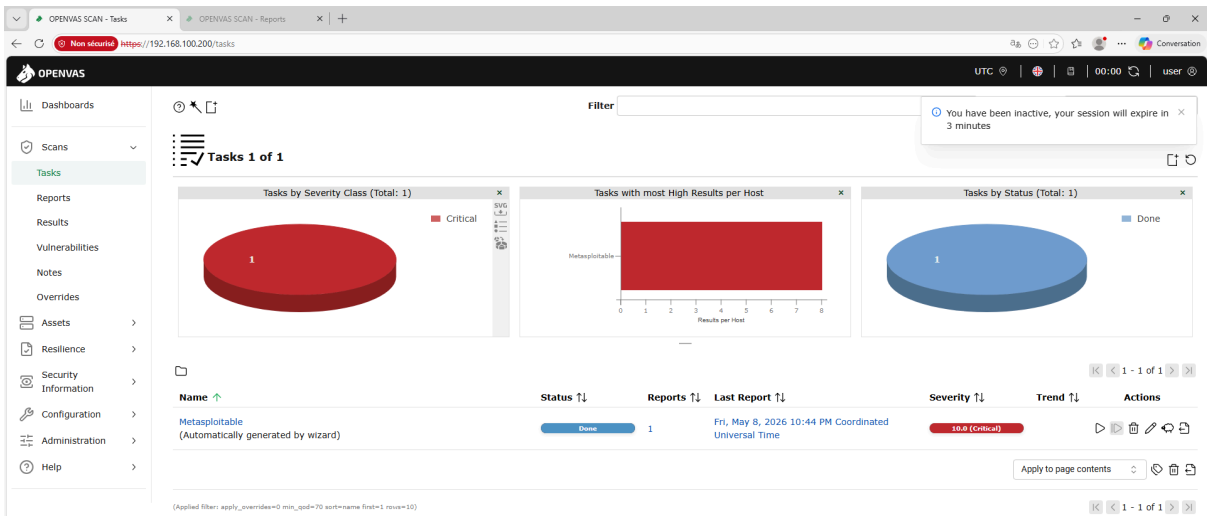
Consultation du rapport généré après l'analyse de la machine Metasploitable.



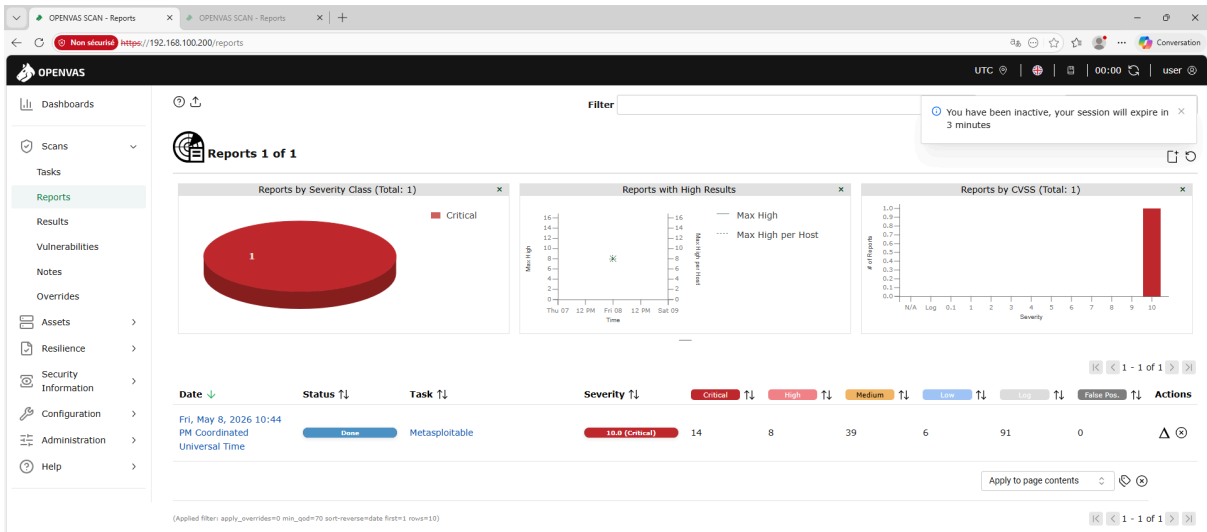
Analyse des résultats du scan Metasploitable montrant les vulnérabilités détectées et leur niveau de sévérité.



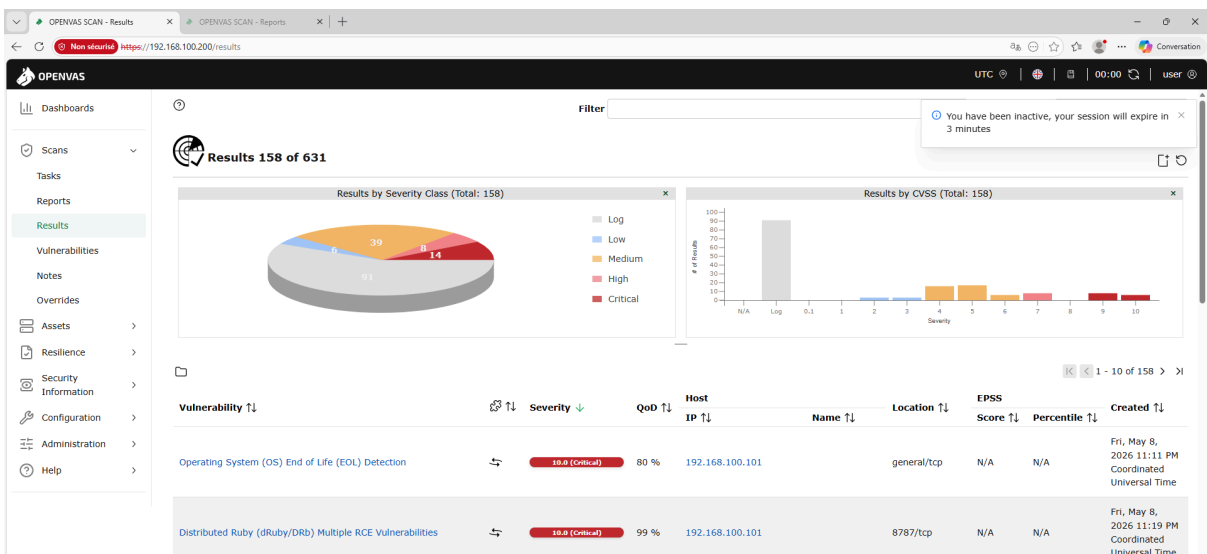
Consultation du tableau de bord des tâches OpenVAS après la fin du scan de sécurité.



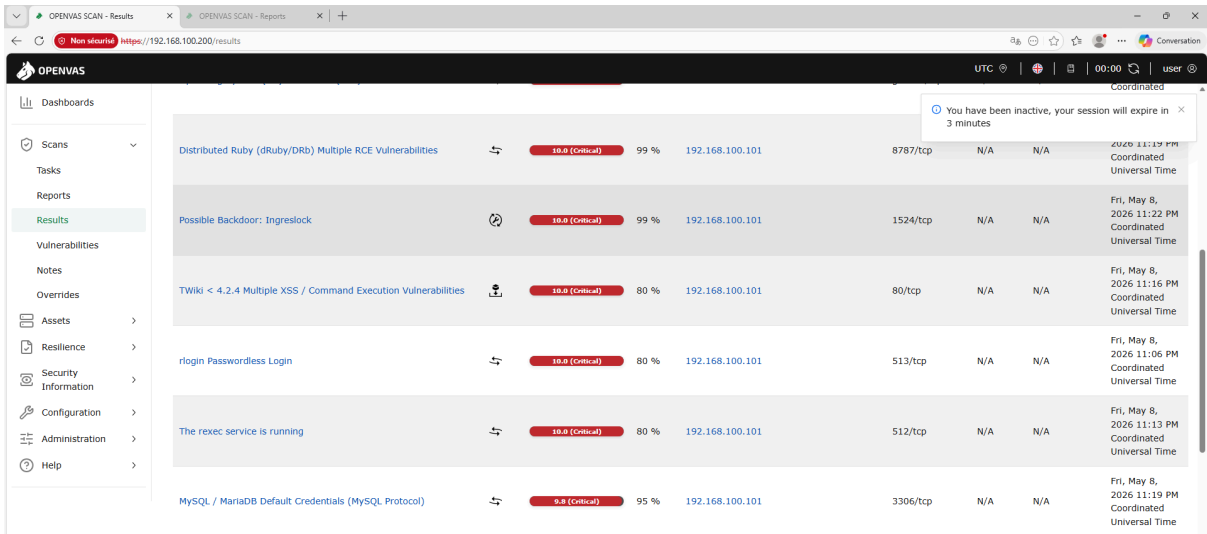
Affichage du rapport final du scan Metasploitable avec un score de sévérité critique détecté par OpenVAS.



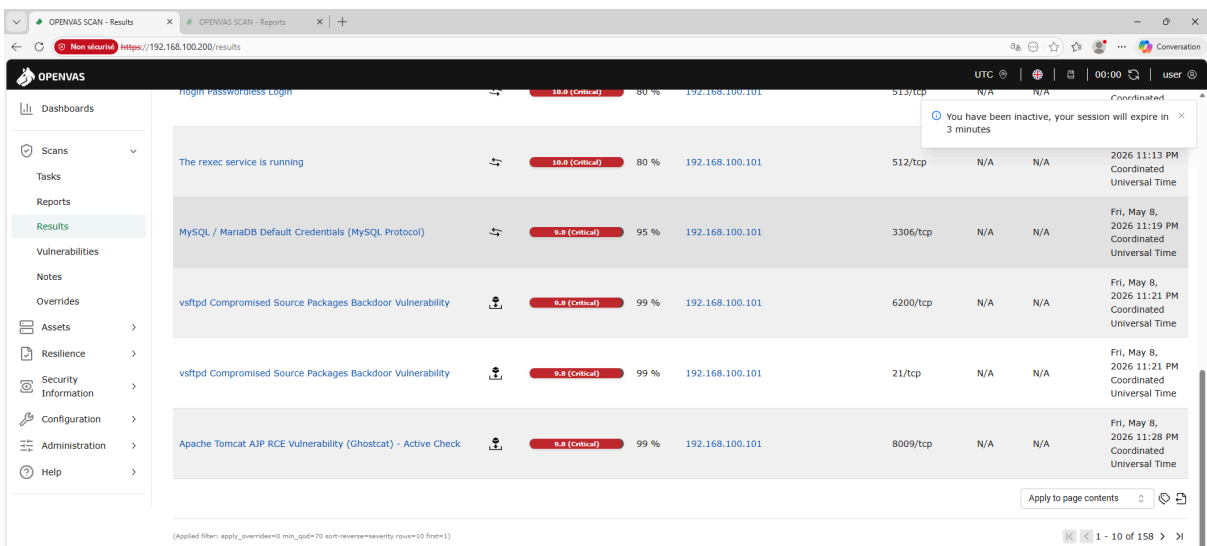
Consultation détaillée des vulnérabilités détectées, des ports ouverts et des scores CVSS associés.



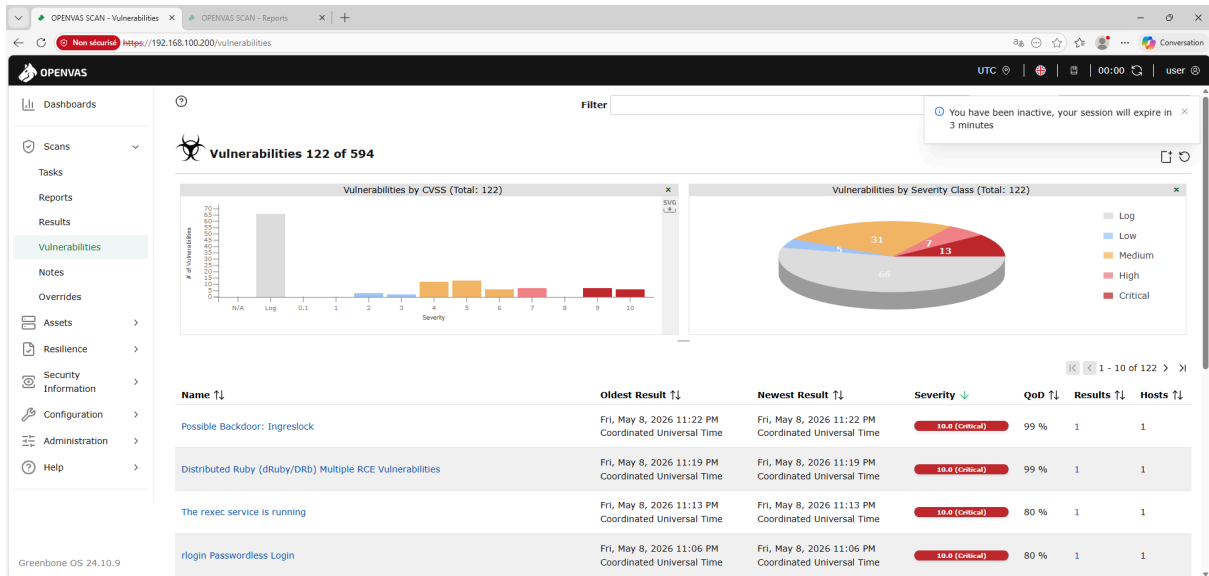
Affichage des vulnérabilités critiques détectées sur la machine Metasploitable après l'analyse OpenVAS.



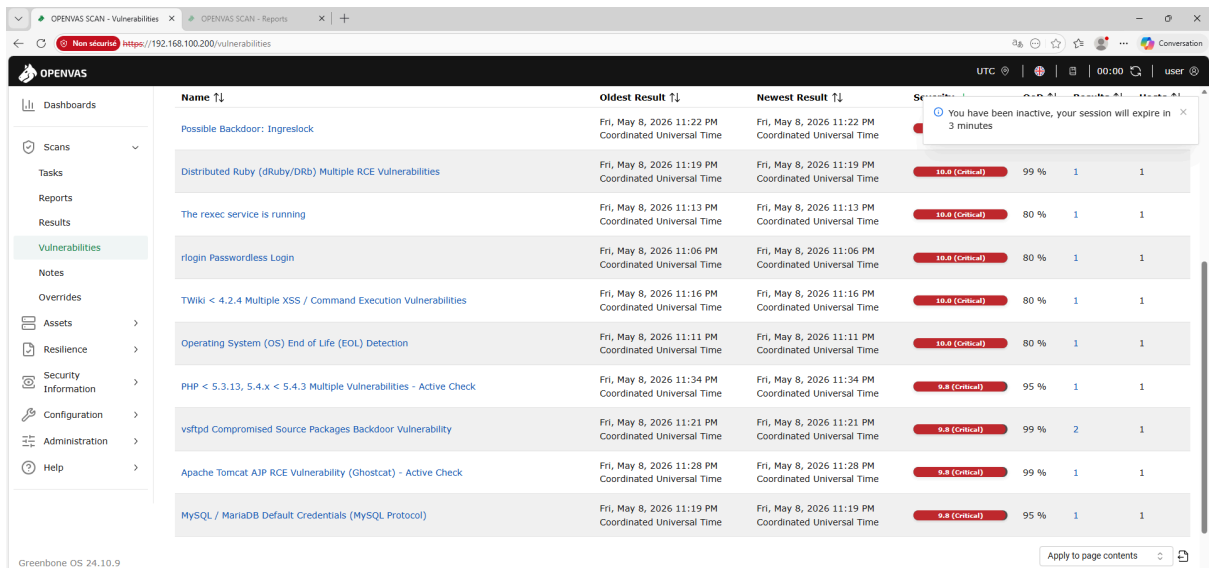
Consultation détaillée des failles de sécurité identifiées avec leurs niveaux de criticité et services associés.



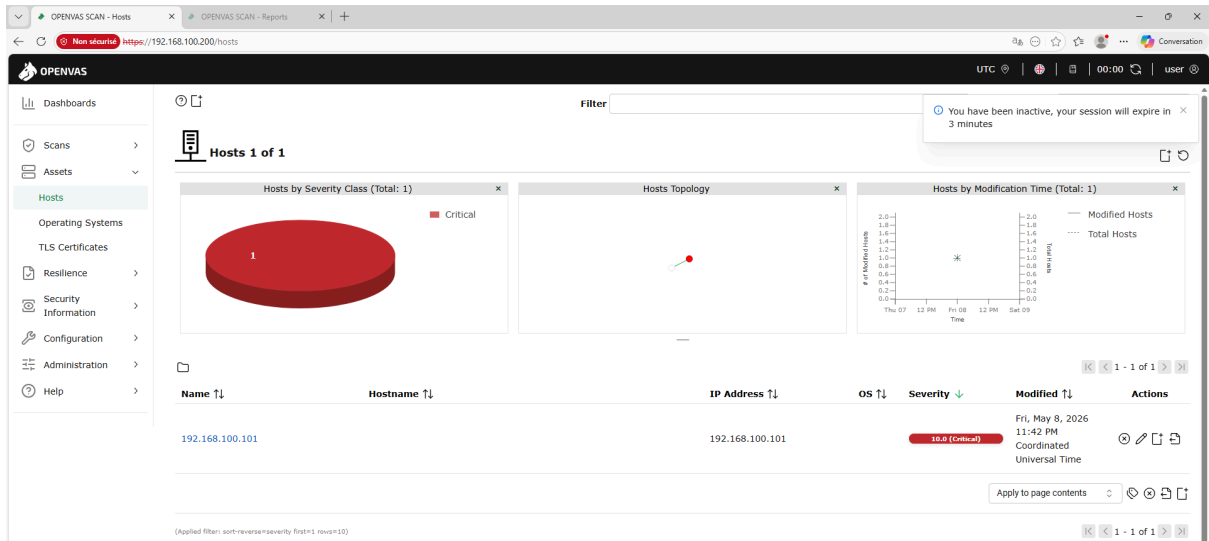
Affichage de la liste des vulnérabilités détectées par OpenVAS avec leur niveau de sévérité.



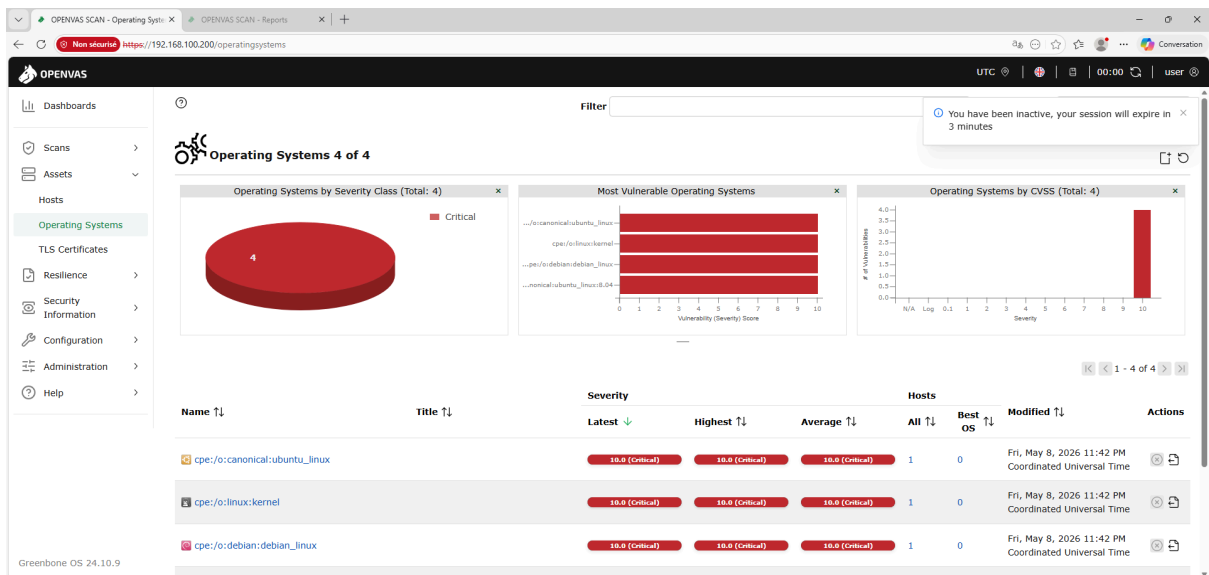
Analyse détaillée des failles de sécurité critiques présentes sur la machine Metasploitable.



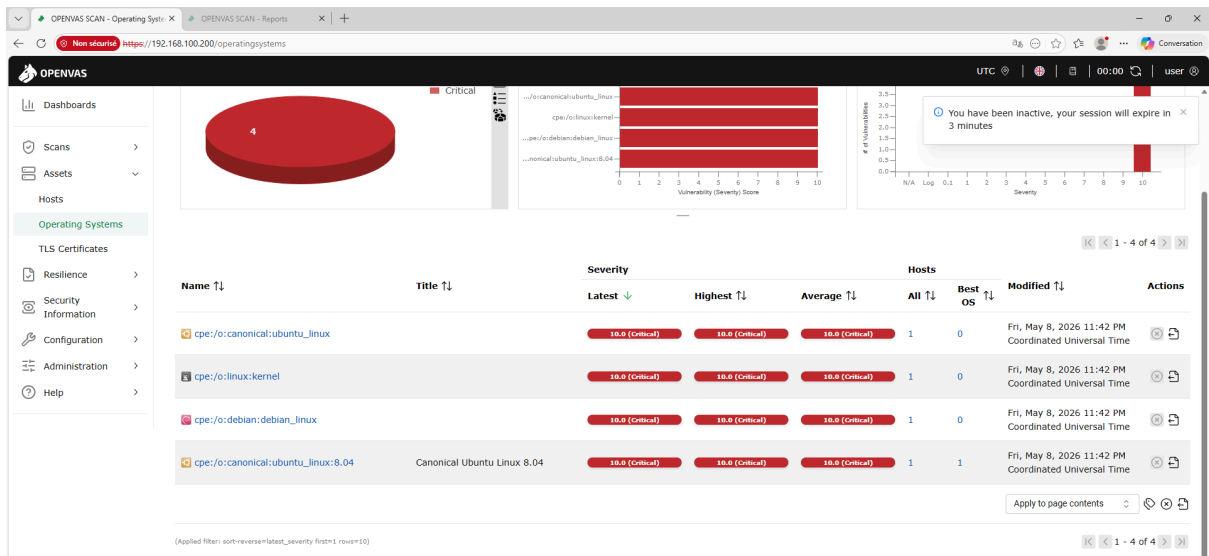
Consultation des informations sur l'hôte analysé, notamment l'adresse IP et le niveau de sévérité détecté.



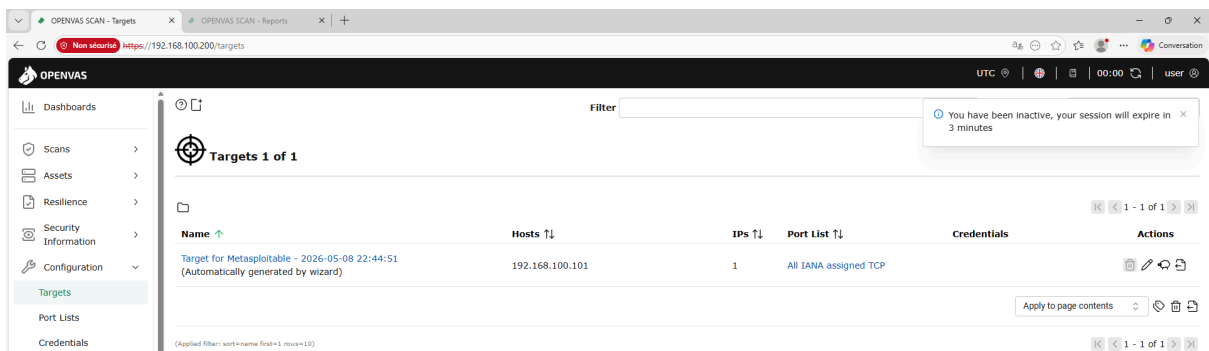
Identification des systèmes d'exploitation détectés par OpenVAS lors du scan de vulnérabilités.



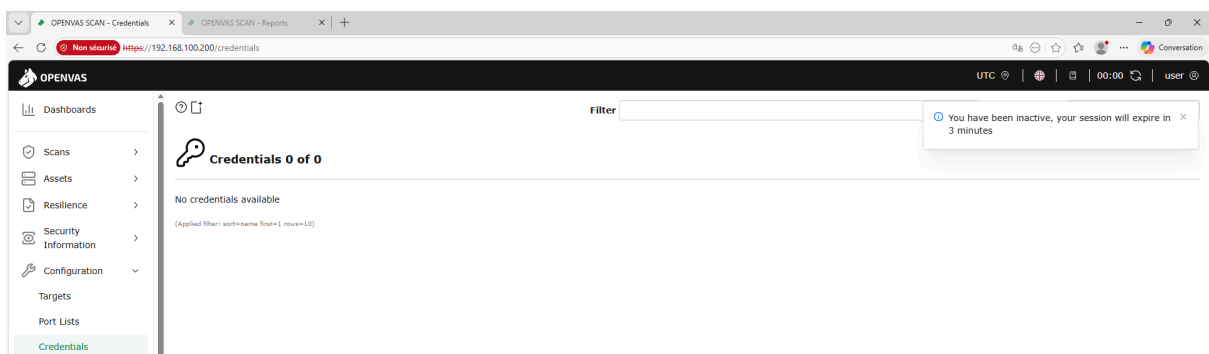
Affichage des systèmes d'exploitation détectés et de leur niveau de criticité associé.



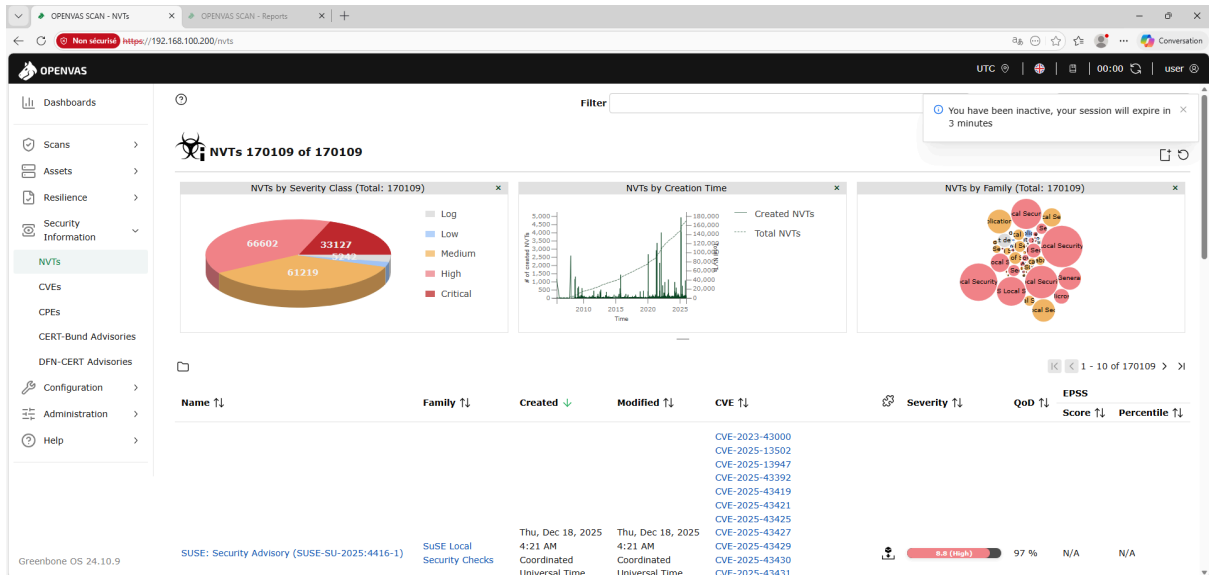
Consultation de la cible configurée dans OpenVAS pour le scan de la machine Metasploitable.



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



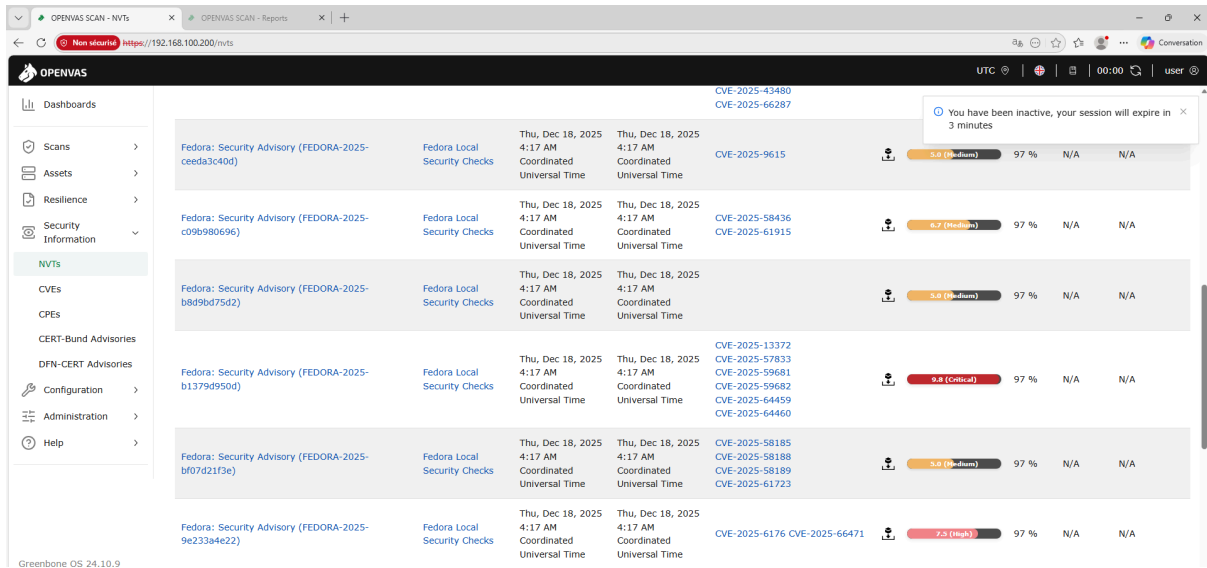
Consultation des NVTs (Network Vulnerability Tests) utilisés par OpenVAS pour détecter les vulnérabilités.



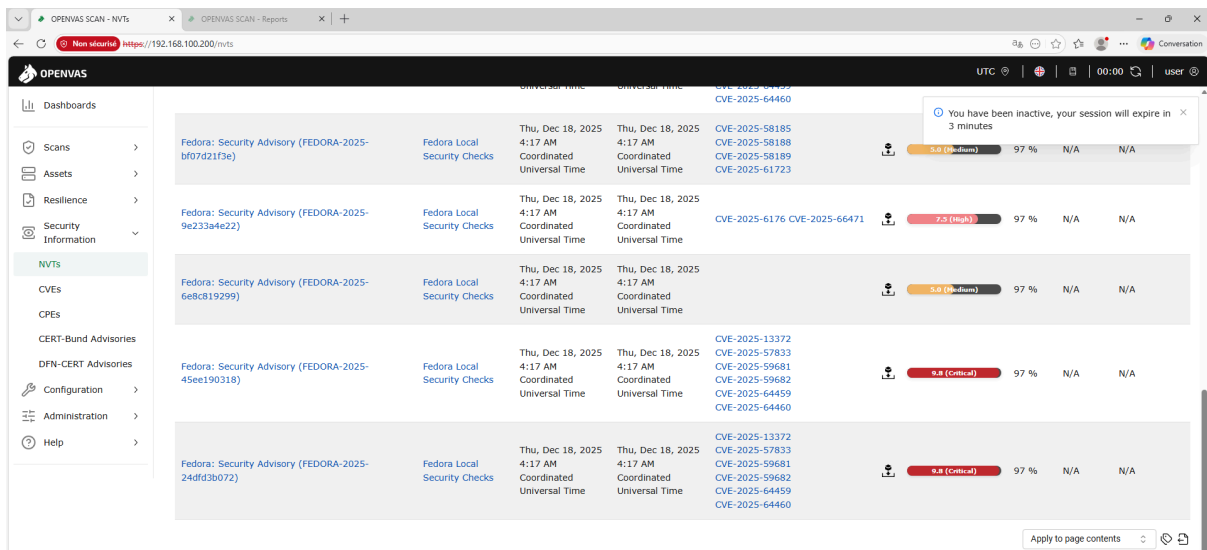
Affichage détaillé des signatures de vulnérabilités et des CVE associées détectées pendant le scan.

Name	Family	Created	Modified	CVE	Severity	QoD	EPSS Score	Percentile
SUSE: Security Advisory (SUSE-SU-2025:4416-1)					8.8 (High)	97 %	N/A	N/A
Fedora: Security Advisory (FEDORA-2025-c9b980696)					5.0 (Medium)	97 %	N/A	N/A
Fedora: Security Advisory (FEDORA-2025-c09b980696)					6.2 (Medium)	97 %	N/A	N/A

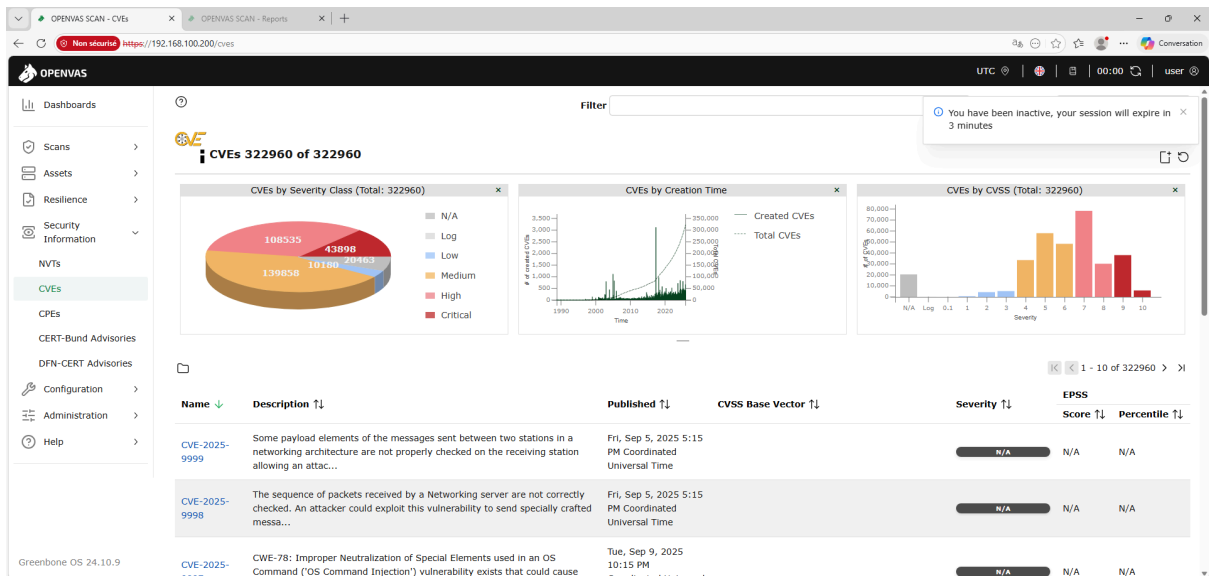
Consultation des avis de sécurité et des vulnérabilités référencées dans les bases NVT de Greenbone.



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.

CVE ID	Description	Published	CVSS Base Vector	Severity	EPSS Score	Percentile
CVE-2025-9997	CWE-78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection") vulnerability exists that could cause command injection in BL...	Tue, Sep 9, 2025 10:15 PM Coordinated Universal Time		N/A	N/A	N/A
CVE-2025-9996	CWE-78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection") vulnerability exists that could cause the execution of any sh...	Tue, Sep 9, 2025 9:15 PM Coordinated Universal Time		N/A	N/A	N/A
CVE-2025-9994	The Amp'ed RF BT-AP 111 Bluetooth access point's HTTP admin interface does not have an authentication feature, allowing unauthorized access to anyone with netwo...	Tue, Sep 9, 2025 2:15 PM Coordinated Universal Time	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8 (Critical)	N/A	N/A
CVE-2025-9993	The Bei Fen - WordPress Backup Plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.4.2 via the 'task'. Thi...	Tue, Sep 30, 2025 11:37 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	9.1 (High)	N/A	N/A
CVE-2025-9992	The Ghost Kit - Page Builder Blocks, Motion Effects & Extensions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom JS field in al...	Thu, Sep 18, 2025 10:15 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N	6.4 (Medium)	N/A	N/A
CVE-2025-9991	The Tiny Bootstrap Elements Light plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.3.34 via the 'language' par...	Tue, Sep 30, 2025 11:37 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	9.1 (High)	N/A	N/A
CVE-2025-9990	The WordPress Helpdesk Integration plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.8.10 via the portal_type p...	Fri, Sep 5, 2025 3:15 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	9.1 (High)	N/A	N/A
CVE-2025-9989	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.2.7	Fri, Sep 26, 2025 5:15 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3 (Medium)	N/A	N/A

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

The screenshot shows the OpenVAS interface with a list of CVEs. The left sidebar contains navigation options like Dashboards, Scans, Assets, Resilience, Security Information, NVTs, CVEs, CPEs, and Advisories. The main content area displays a table of CVEs with columns for ID, description, date, and severity. A session expiration warning is visible in the top right corner.

CVE ID	Description	Date	Severity
CVE-2025-9994	The Amp'ed RF BT-AP 111 Bluetooth access point's HTTP admin interface does not have an authentication feature, allowing unauthorized access to anyone with netwo...	Tue, Sep 9, 2025 2:15 PM Coordinated Universal Time	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C/H/I:H
CVE-2025-9993	The Bel Fen - WordPress Backup Plugin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.4.2 via the 'task'. Thi...	Tue, Sep 30, 2025 11:37 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C/H/I:H/A:H 8.1 (High)
CVE-2025-9992	The Ghost Kit - Page Builder Blocks, Motion Effects & Extensions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom JS field in al...	Thu, Sep 18, 2025 10:15 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C/L/I:L/A:N 6.4 (Medium)
CVE-2025-9991	The Tiny Bootstrap Elements Light plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.3.34 via the 'language' par...	Tue, Sep 30, 2025 11:37 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C/H/I:H/A:H 8.1 (High)
CVE-2025-9990	The WordPress Helpdesk Integration plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.8.10 via the portal_type p...	Fri, Sep 5, 2025 3:15 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C/H/I:H/A:H 8.1 (High)
CVE-2025-9985	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.2.7 through publ...	Fri, Sep 26, 2025 5:15 AM Coordinated Universal Time	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C/L/I:N/A:N 5.3 (Medium)

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

The screenshot shows the OpenVAS CPEs page. It features a summary of 1530345 CPEs, broken down by severity class (Critical, High, Medium, Low, Log, N/A) and a chart showing CPEs by creation time. Below the charts is a table listing specific CPEs for IBM UrbanCode Deploy.

Name	Title	Modified	CVEs	Severity
cpe:/a:ibm:urbancode_deploy:7.3.0.1	IBM UrbanCode Deploy 7.3.0.1	Wed, Dec 17, 2025 8:50 PM Coordinated Universal Time	0	N/A
cpe:/a:ibm:urbancode_deploy:7.1.2.28	IBM UrbanCode Deploy 7.1.2.28	Wed, Dec 17, 2025 8:50 PM Coordinated Universal Time	0	N/A
cpe:/a:ibm:urbancode_deploy:7.2.3.21	IBM UrbanCode Deploy 7.2.3.21	Wed, Dec 17, 2025 8:50 PM Coordinated Universal Time	0	N/A
cpe:/a:ibm:urbancode_deploy:7.3.2.16	IBM UrbanCode Deploy 7.3.2.16	Wed, Dec 17, 2025 8:50 PM Coordinated Universal Time	0	N/A

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

The screenshot shows the 'CPEs' section of the OpenVAS interface. It displays a table of detected software packages. The table has columns for CPE identifier, product name, version, and other details. The packages listed are all instances of IBM UrbanCode Deploy with various versions and CPE identifiers.

CPE Identifier	Product Name	Version	Other Info
cpe:/a:ibm:urbancode_deploy:7.3.0.1	IBM UrbanCode Deploy	7.3.0.1	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:7.1.2.28	IBM UrbanCode Deploy	7.1.2.28	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:7.2.3.21	IBM UrbanCode Deploy	7.2.3.21	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:7.3.2.16	IBM UrbanCode Deploy	7.3.2.16	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:2.6.0	IBM UrbanCode Deploy	2.6.0	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:6.0.1.14	IBM UrbanCode Deploy	6.0.1.14	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:6.0.1.15	IBM UrbanCode Deploy	6.0.1.15	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:6.1.0.10	IBM UrbanCode Deploy	6.1.0.10	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:6.1.3.9	IBM UrbanCode Deploy	6.1.3.9	Wed, 17 Dec 2025 8:50 PM
cpe:/a:ibm:urbancode_deploy:6.2.7.8	IBM UrbanCode Deploy	6.2.7.8	Wed, 17 Dec 2025 8:50 PM

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

The screenshot shows the 'CERT-Bund Advisories' section of the OpenVAS interface. It features a summary of 25185 advisories, including three charts: a pie chart for severity classes, a line chart for creation time, and a bar chart for CVSS scores. Below the charts is a table of specific advisories.

CERT-Bund Advisories 25185 of 25185

CERT-Bund Advisories by Severity Class (Total: 25185)

Severity Class	Count
N/A	10586
Low	1972
Medium	7348
High	5196
Critical	0

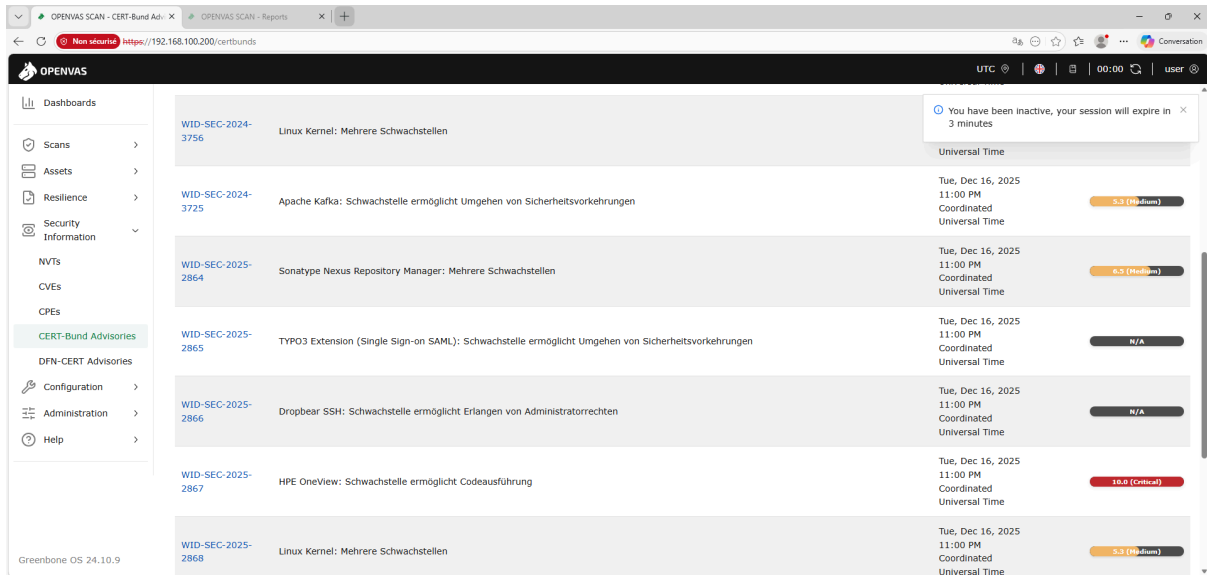
CERT-Bund Advisories by Creation Time

CERT-Bund Advisories by CVSS (Total: 25185)

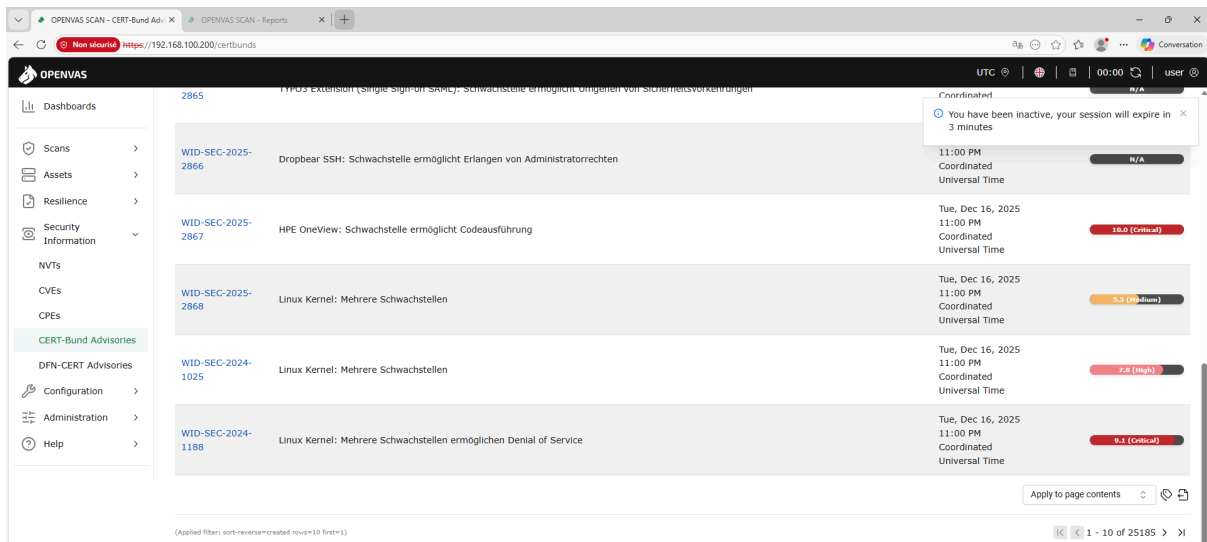
CVSS Score	Count
N/A	~1000
Log	~1000
0.1	~1000
0.2	~1000
0.3	~1000
0.4	~1000
0.5	~1000
0.6	~1000
0.7	~1000
0.8	~1000
0.9	~1000
1.0	~1000

Name	Title	Created	CVES	Severity
WID-SEC-2024-3762	Linux Kernel: Mehrere Schwachstellen ermöglichen Denial of Service	Tue, Dec 16, 2025 11:00 PM	Coordinated Universal Time	7.8 (High)
WID-SEC-2024-3756	Linux Kernel: Mehrere Schwachstellen	Tue, Dec 16, 2025 11:00 PM	Coordinated Universal Time	7.8 (High)
WID-SEC-2024-		Tue, Dec 16, 2025 11:00 PM		

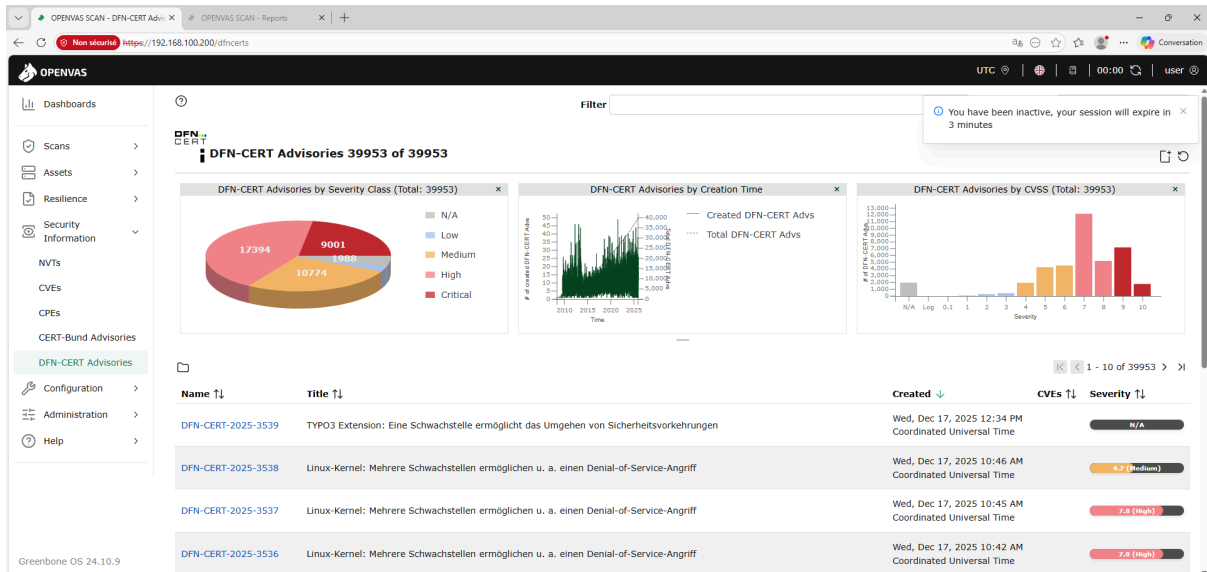
Affichage détaillé des avis CERT-Bund et des niveaux de sévérité associés aux vulnérabilités détectées.



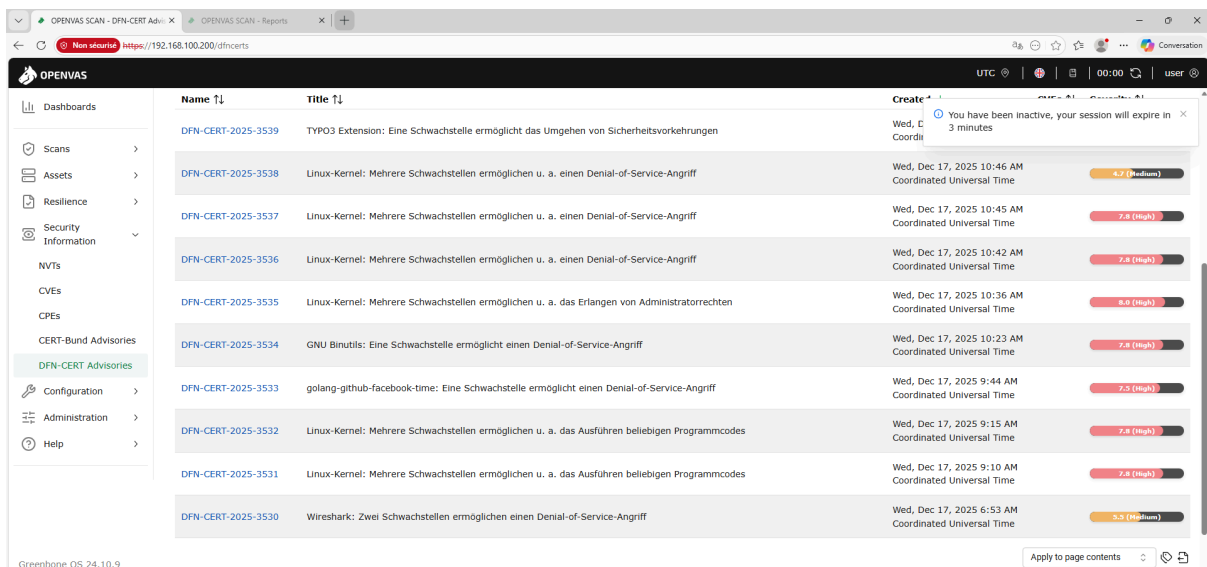
Consultation des recommandations de sécurité publiées par les organismes CERT concernant les failles identifiées.



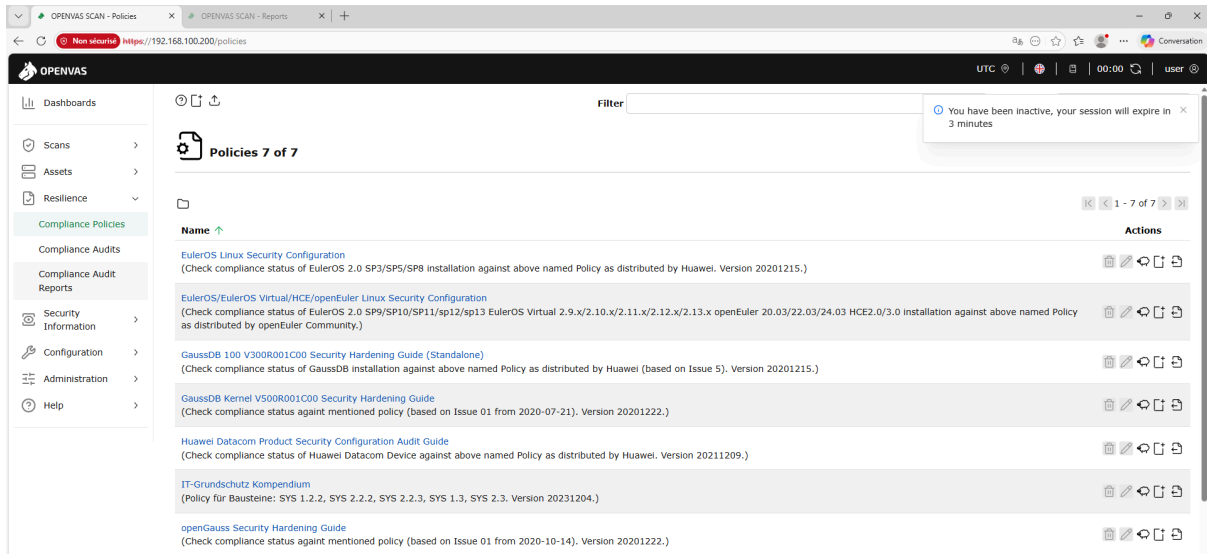
Consultation des avis DFN-CERT liés aux vulnérabilités détectées par OpenVAS.



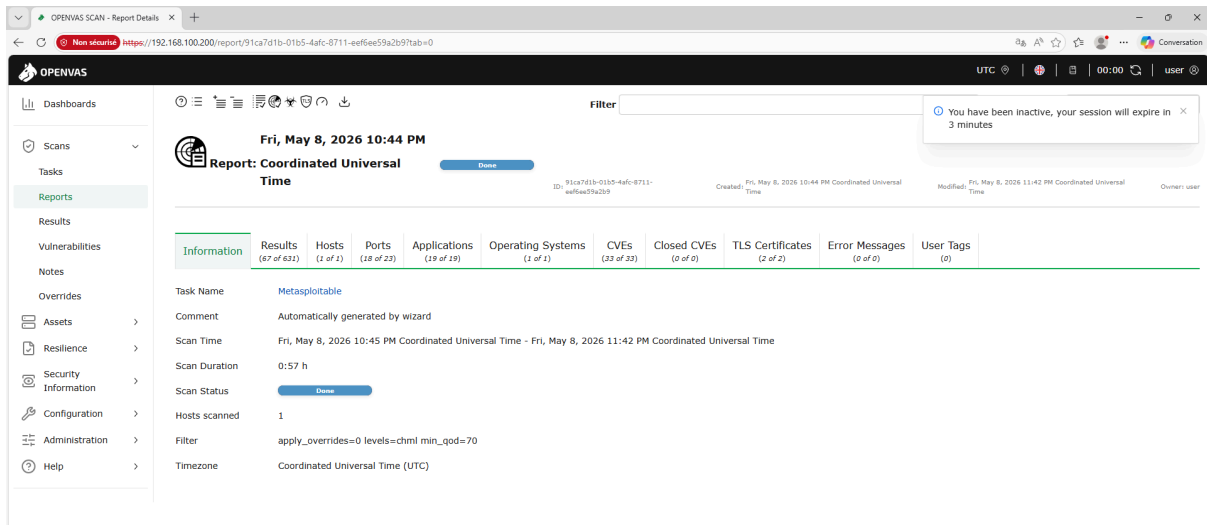
Analyse détaillée des alertes DFN-CERT et des niveaux de criticité associés aux failles de sécurité identifiées.



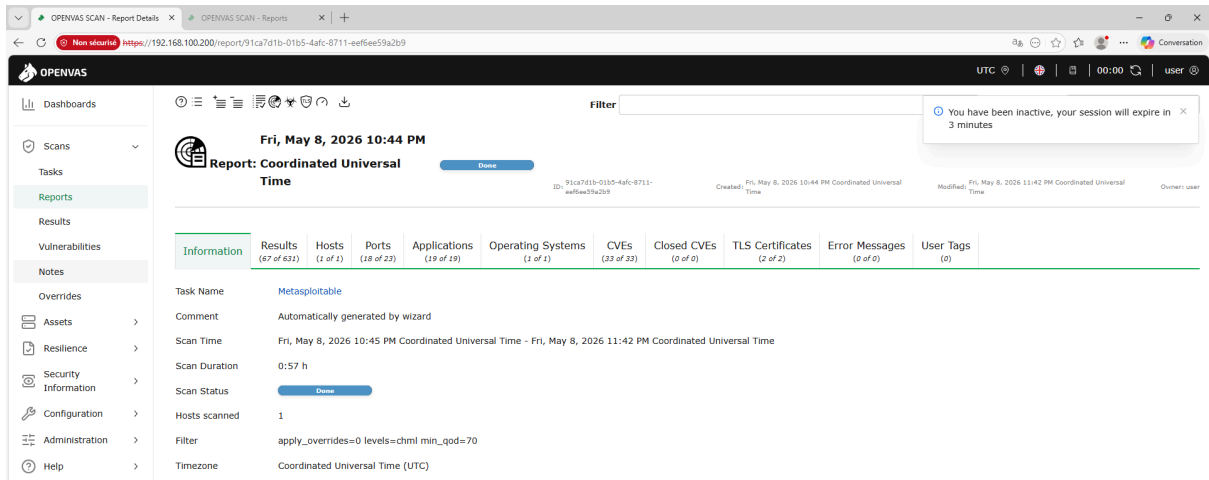
Consultation des politiques de conformité et des modèles d'audit de sécurité disponibles dans OpenVAS.



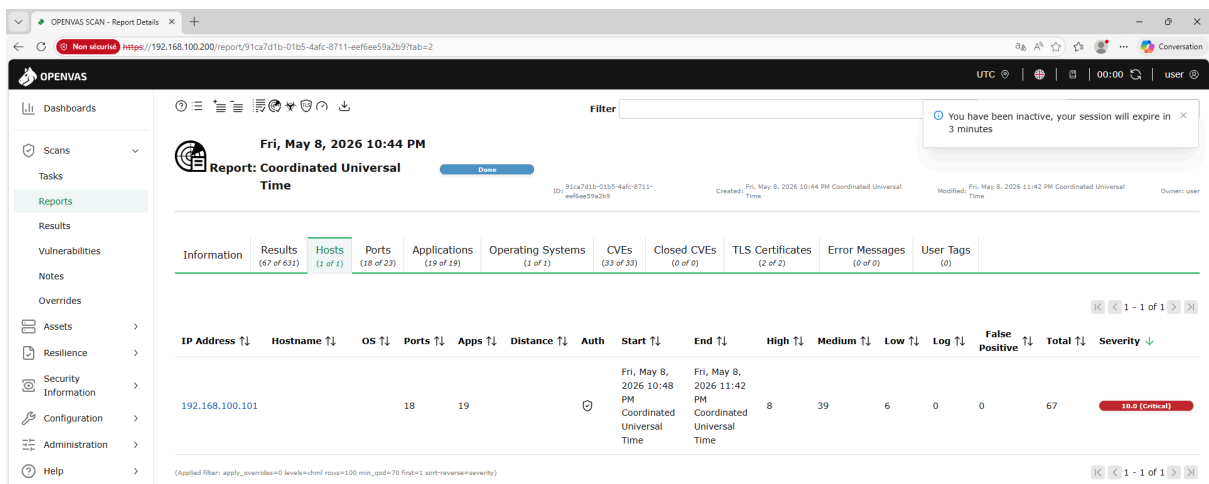
Affichage du rapport général du scan contenant les informations principales de l'analyse de vulnérabilités.



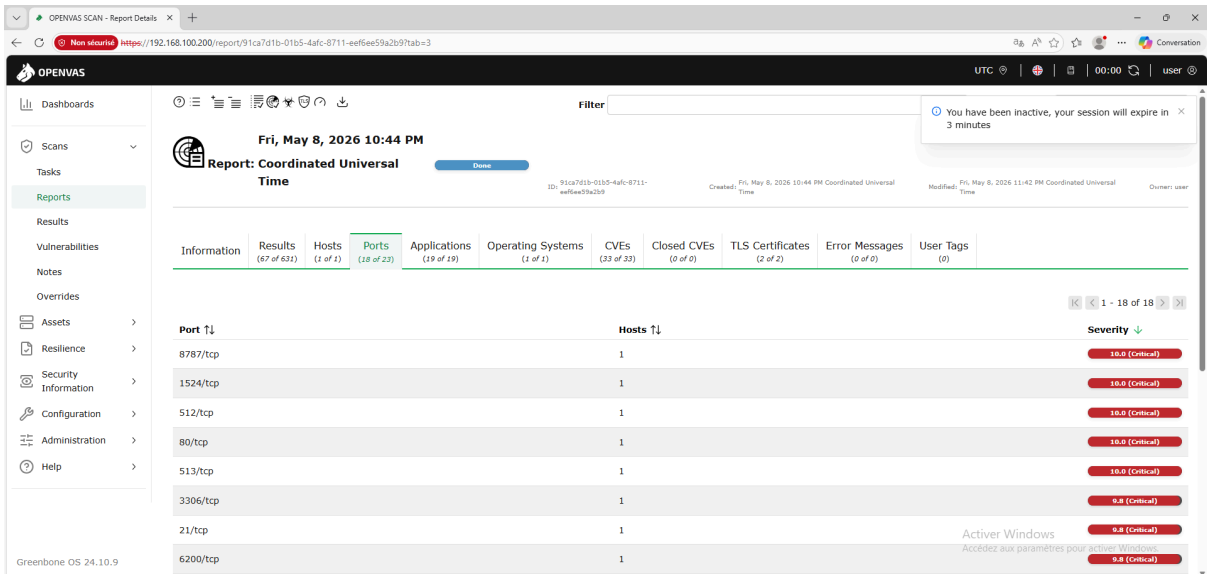
Consultation des informations générales du rapport de scan généré par OpenVAS.



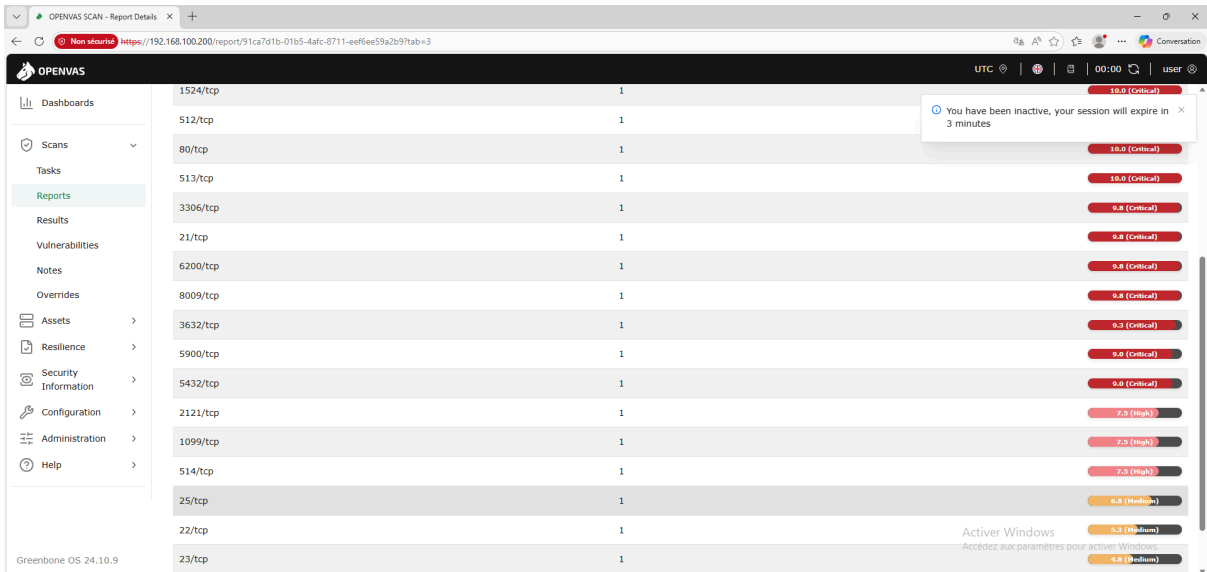
Affichage du résumé des résultats du scan avec le nombre de vulnérabilités détectées et le score de sévérité global.



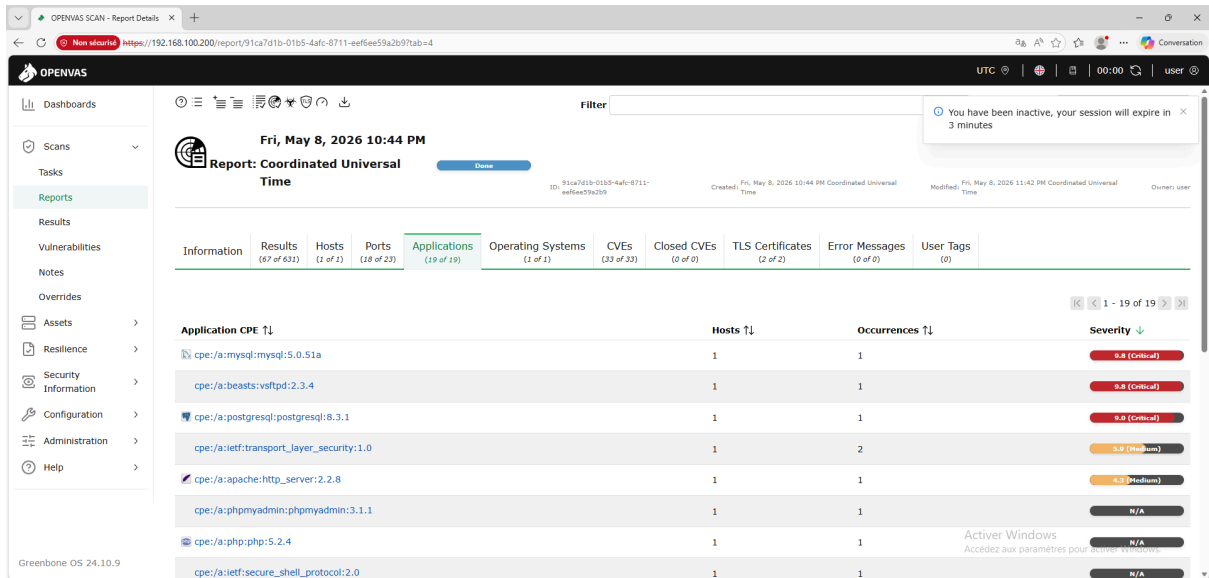
Consultation des ports ouverts détectés sur la machine analysée par OpenVAS.



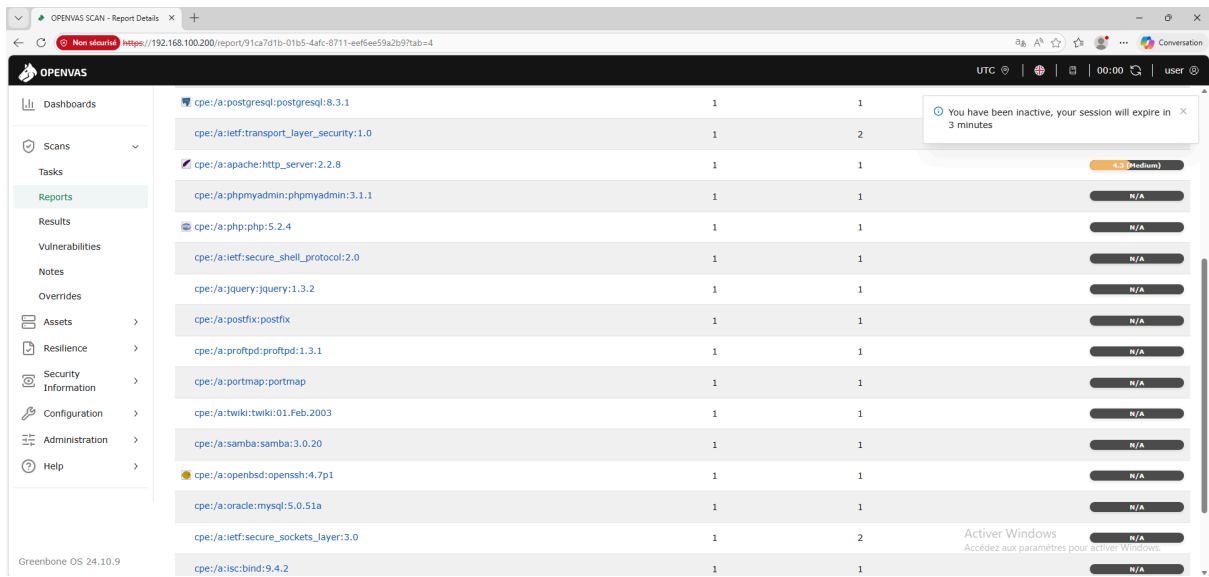
Analyse des services réseau exposés et des niveaux de sévérité associés aux ports détectés.



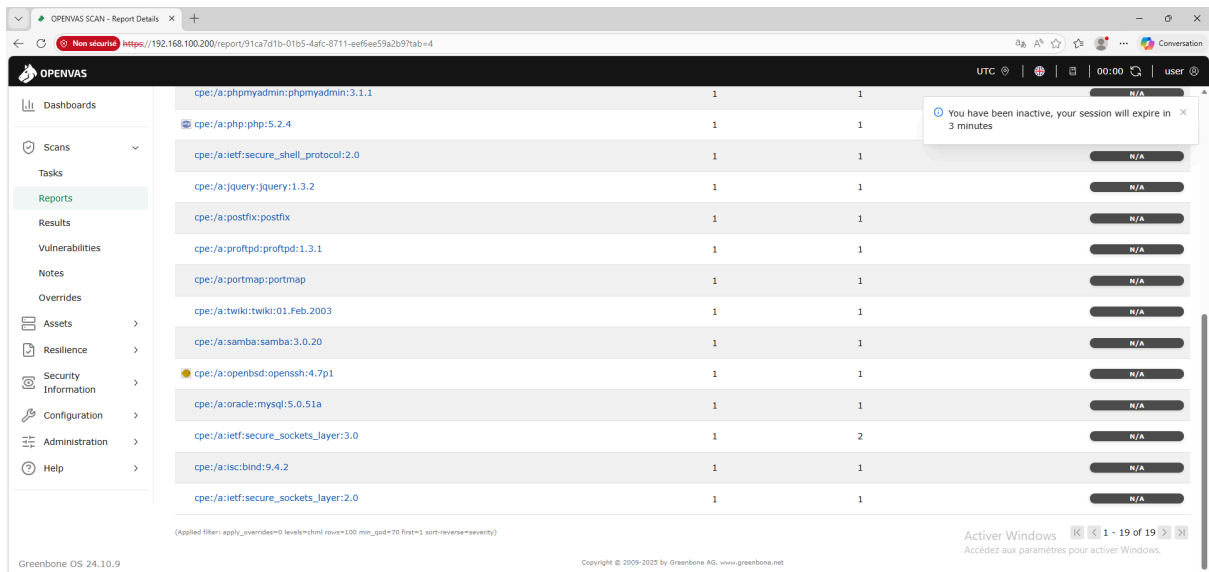
Consultation des applications détectées par OpenVAS sur la machine vulnérable analysée.



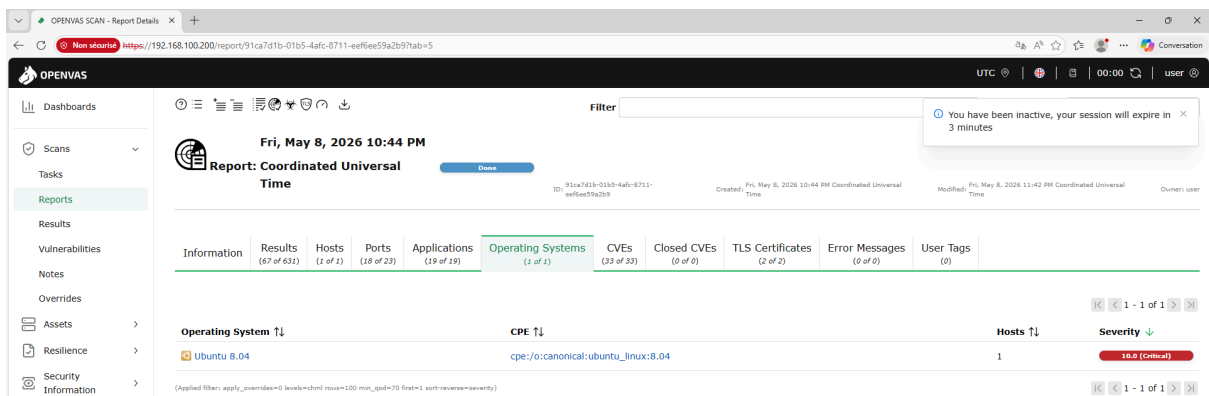
Analyse détaillée des logiciels et composants installés détectés pendant le scan de sécurité.



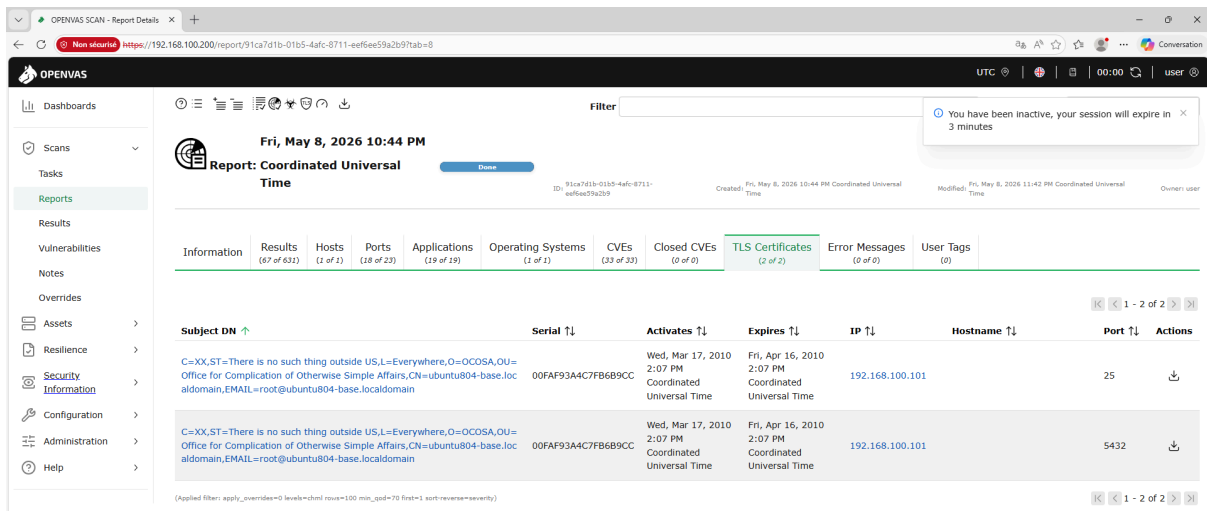
Fin de la liste des applications et composants détectés lors de l'analyse OpenVAS.



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".

Advanced Task Wizard



Quick start: Create a new task

This wizard can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose, whether you want to run the scan immediately or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

For any other setting the defaults from "My Settings" will be applied.

Task Name

Scan Config

Target Host(s)

Start Time
 Start immediately
 Do not start automatically

SSH Credential
 on port

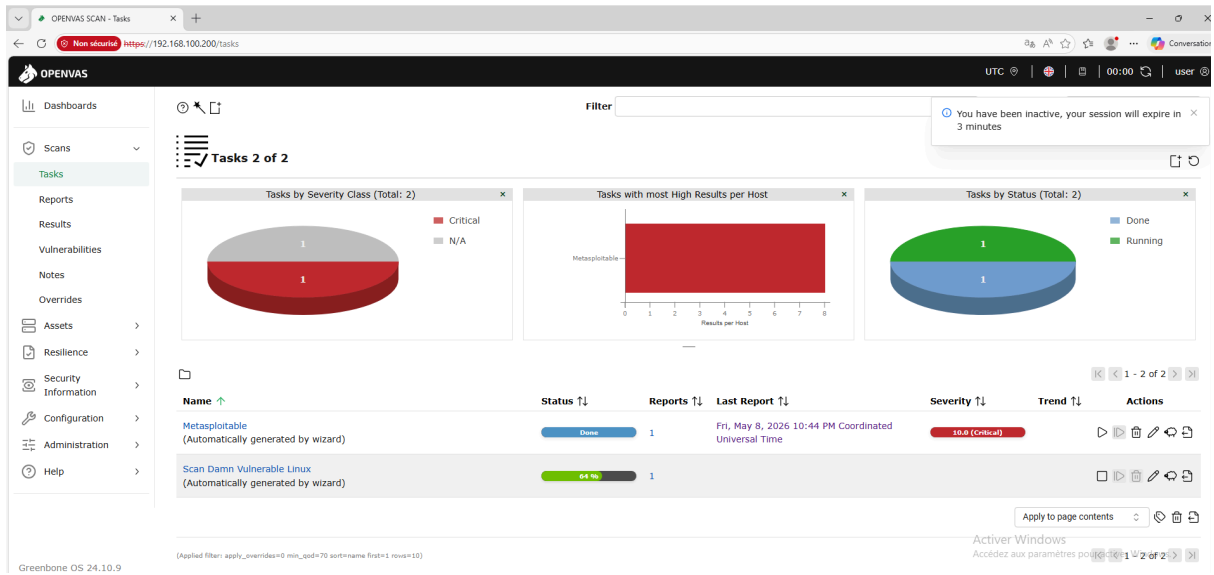
SMB Credential

ESXi Credential

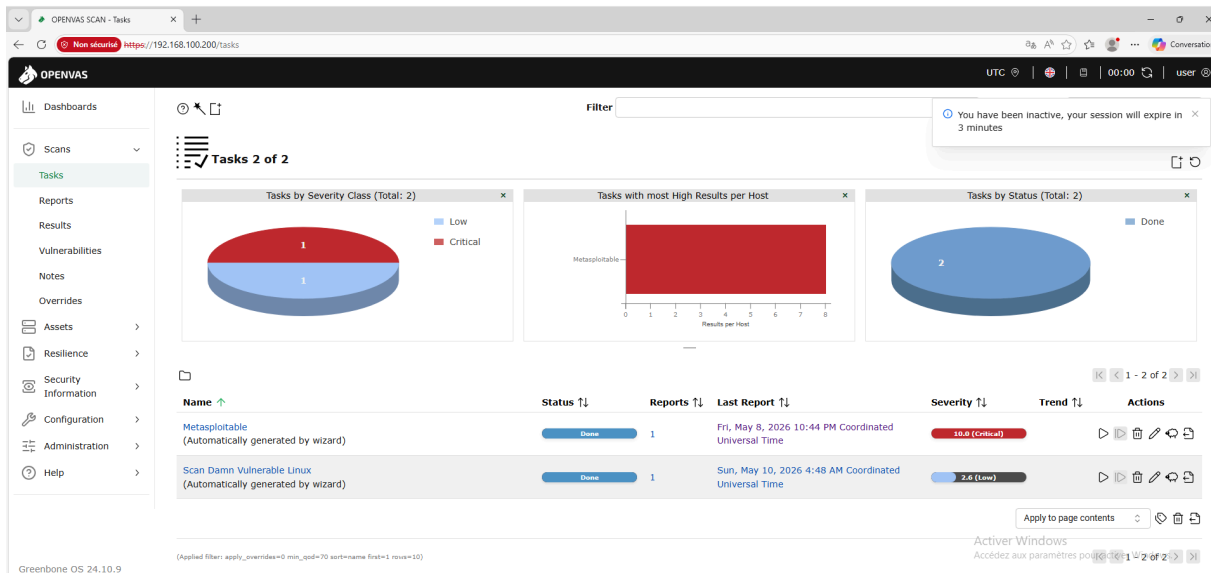
Cancel

Create

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.

The screenshot shows the OpenVAS web interface in a browser. The address bar indicates a non-secure connection to <https://192.168.100.200/task/eca0a5d7-145f-46e7-851b-849927e997cb>. The interface features a sidebar on the left with navigation options: Dashboards, Scans, Tasks (selected), Reports, Results, Vulnerabilities, Notes, Overrides, Assets, Resilience, Security Information, Configuration, Administration, and Help. The main content area displays the task configuration for 'Task: Scan Damn Vulnerable Linux'. It includes tabs for Information, User Tags (0), and Permissions (0). The Information tab is active, showing details such as Name (Scan Damn Vulnerable Linux), Comment (Automatically generated by wizard), Alterable (No), and Status (Done). The Target section shows 'Target for Scan Damn Vulnerable Linux - 2026-05-10 04:48:42'. The Scanner section lists Name (OpenVAS Default), Type (OpenVAS Scanner), and Scan Config (Full and fast). At the bottom, it specifies 'Order for target hosts' and 'Maximum concurrently executed 4 NVTs per host'. The footer of the interface indicates 'Greenbone OS 24.10.9'.

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

The screenshot shows the OpenVAS web interface. The browser address bar indicates the URL: <https://192.168.100.200/task/eca0a5d7-145f-46e7-851b-849927e997cb>. The interface features a sidebar menu on the left with the following items: Dashboards, Scans, Tasks (highlighted), Reports, Results, Vulnerabilities, Notes, Overrides, Assets, Resilience, Security Information, Configuration, Administration, and Help. The main content area is titled 'Scanner' and displays the following configuration details:

- Name:** OpenVAS Default
- Type:** OpenVAS Scanner
- Scan Config:** Full and fast
- Order for target hosts:** Maximum concurrently executed 4 NVTs per host
- Maximum concurrently scanned:** 20 hosts

Below the scanner configuration, the 'Assets' section shows:

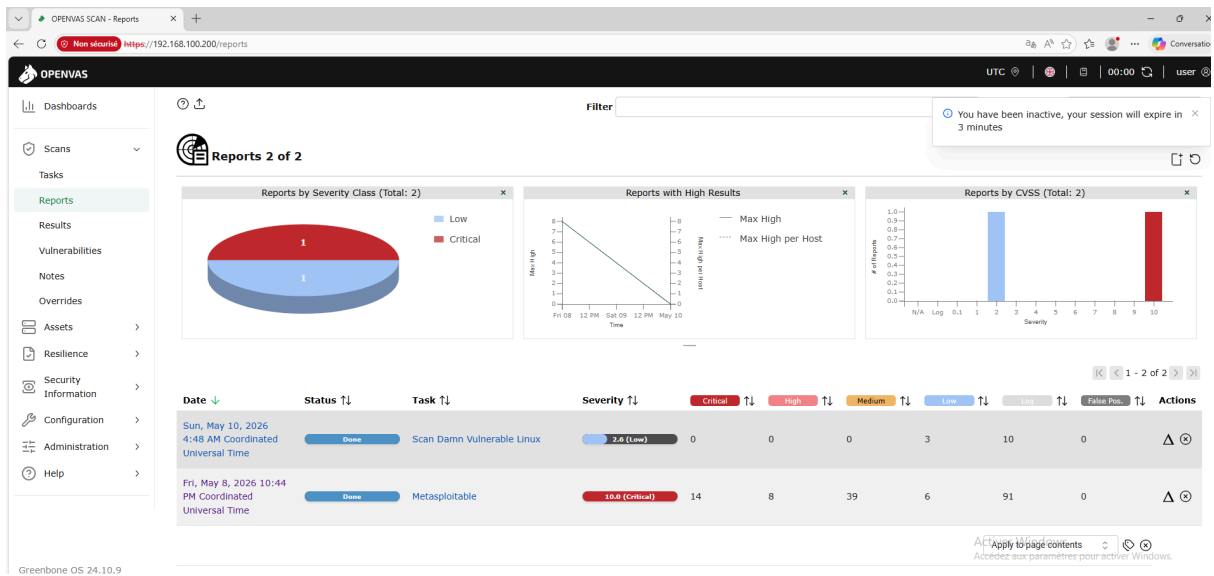
- Add to Assets:** Yes
- Apply Overrides:** Yes
- Min QoD:** 70 %

The 'Scan' section provides the following information:

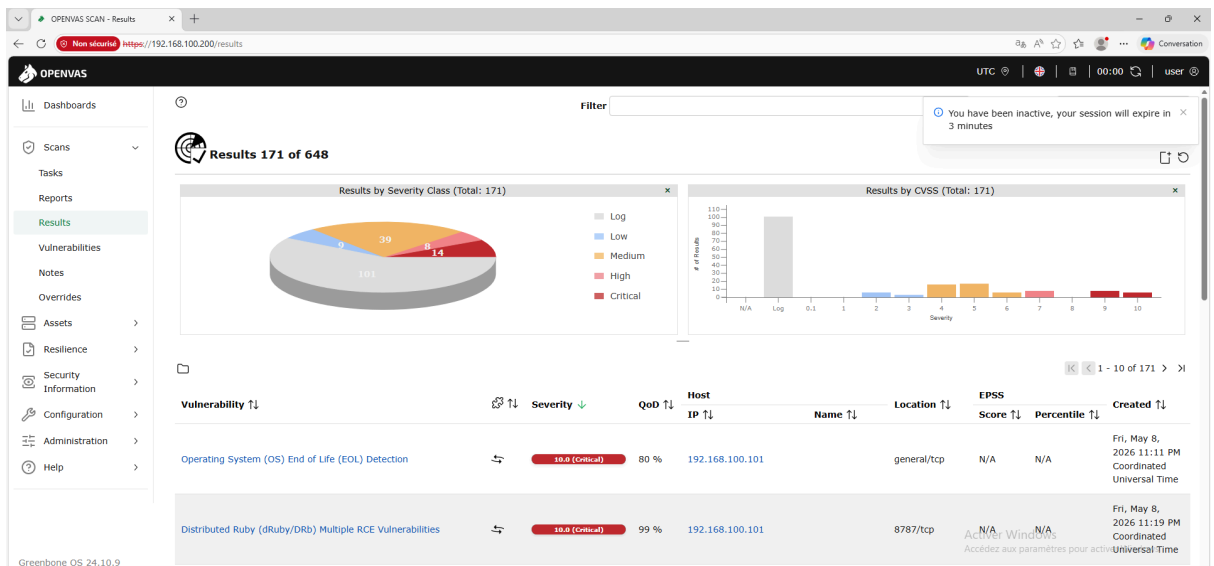
- Duration of last Scan:** 7 minutes
- Average Scan duration:** 7 minutes
- Auto delete Reports:** Do not automatically delete reports

At the bottom left of the interface, the version 'Greenbone OS 24.10.9' is displayed.

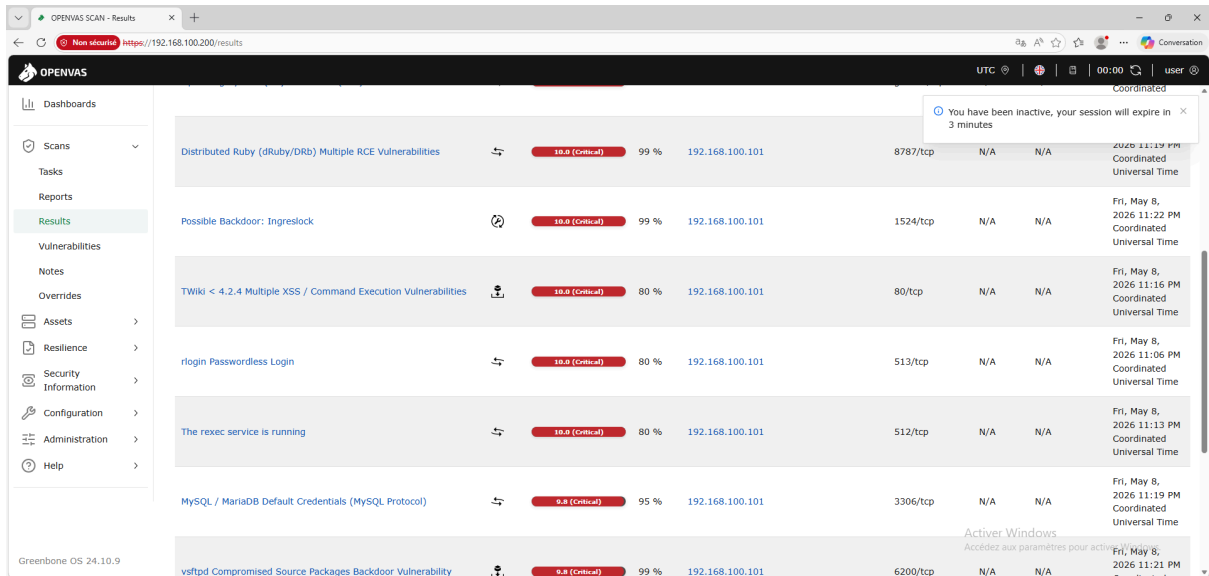
Consultation du rapport final du scan de la machine Damn Vulnerable Linux dans OpenVAS.



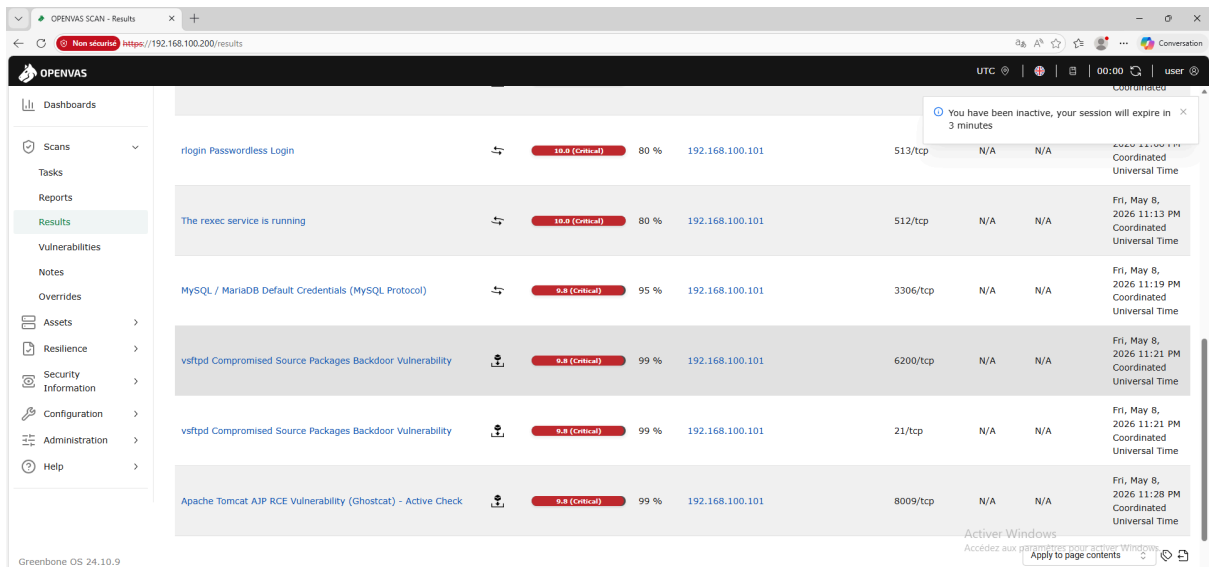
Affichage détaillé des résultats et des vulnérabilités détectées sur Damn Vulnerable Linux.



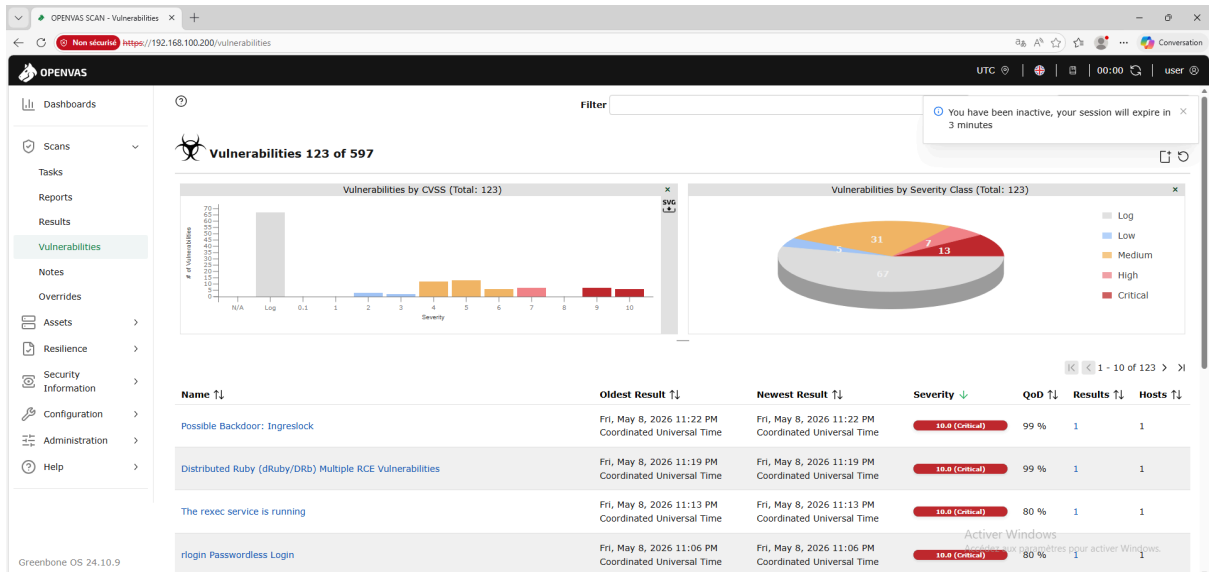
Consultation des vulnérabilités critiques détectées sur la machine Damn Vulnerable Linux.



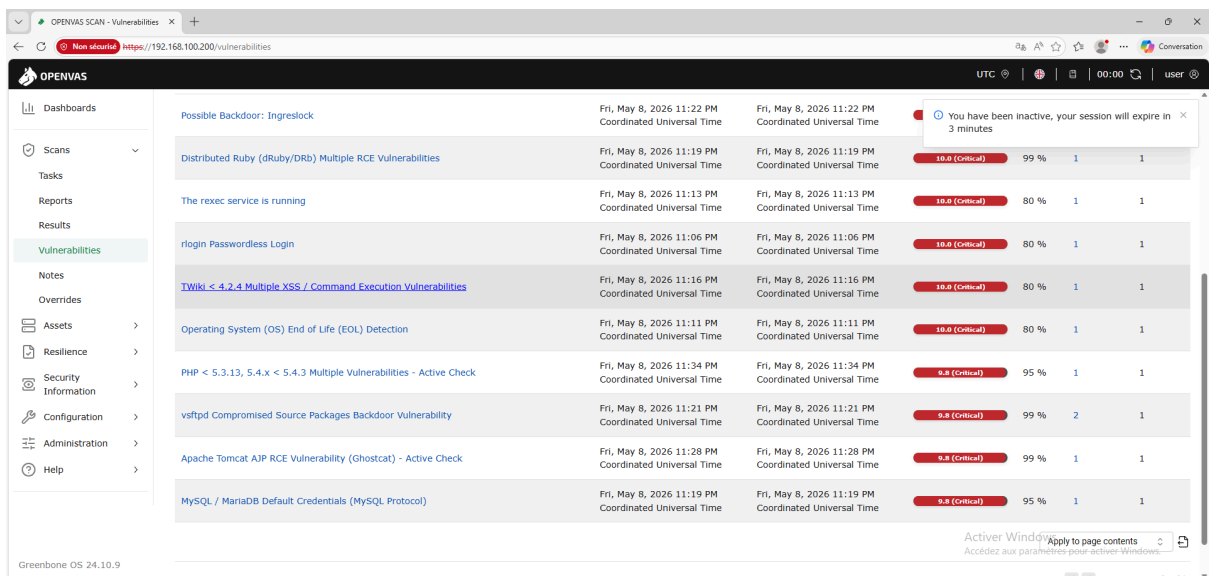
Analyse détaillée des failles de sécurité identifiées avec leurs niveaux de sévérité associés.



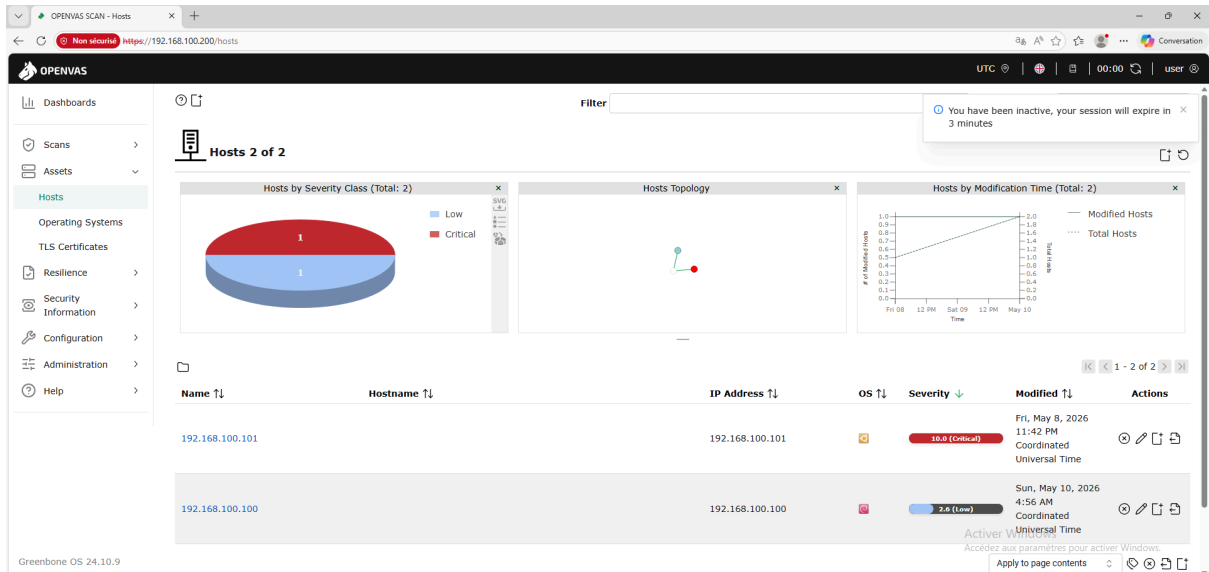
Affichage de la liste des vulnérabilités détectées sur Damn Vulnerable Linux avec leur niveau de criticité.



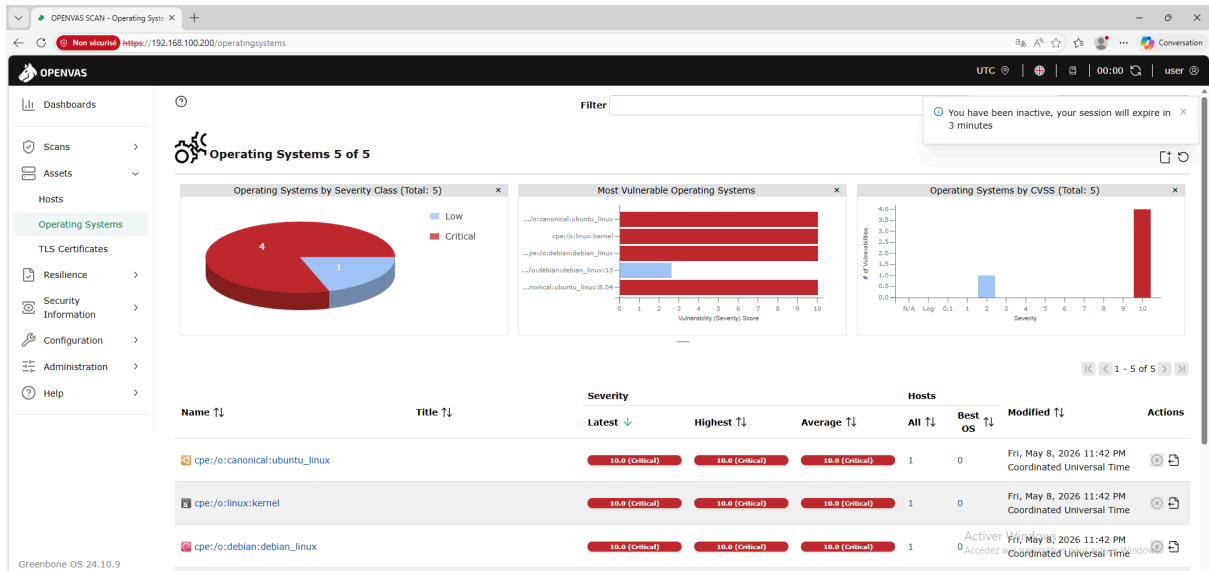
Analyse détaillée des failles de sécurité critiques présentes sur la machine cible analysée.



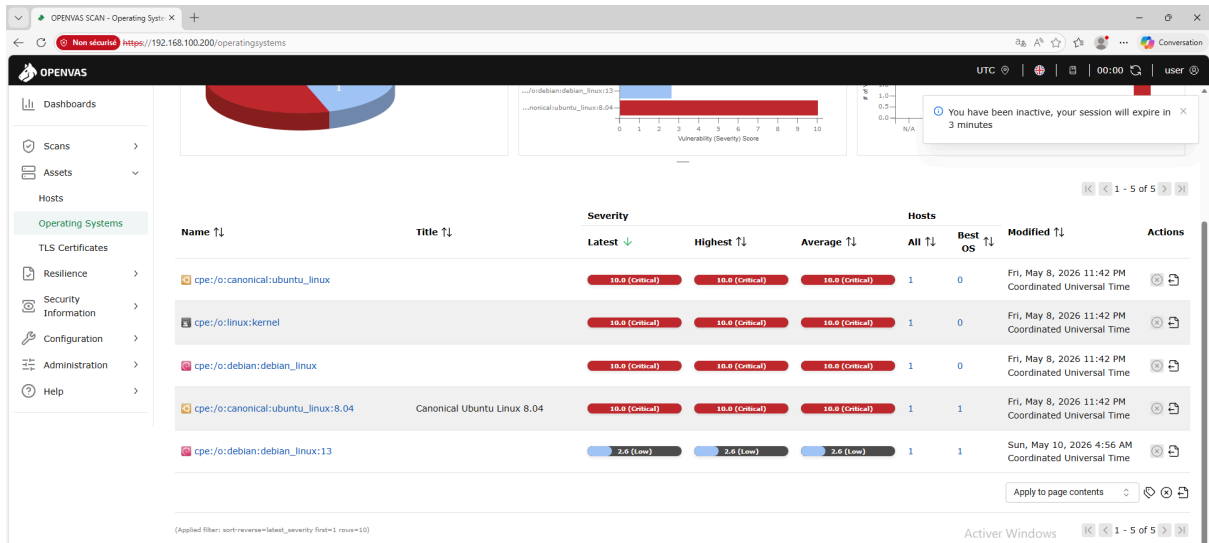
Consultation des hôtes détectés et des niveaux de sévérité associés après le scan de Damn Vulnerable Linux.



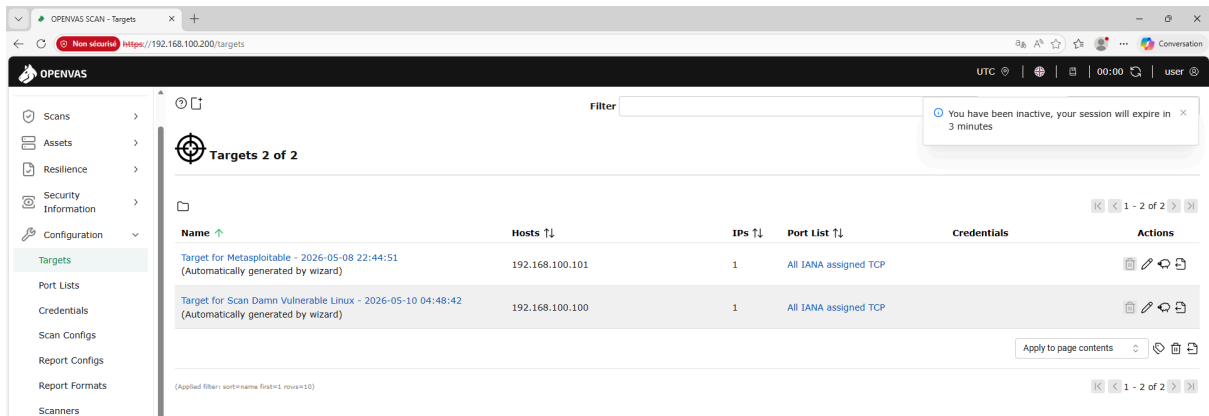
Identification des systèmes d'exploitation détectés automatiquement par OpenVAS lors de l'analyse.



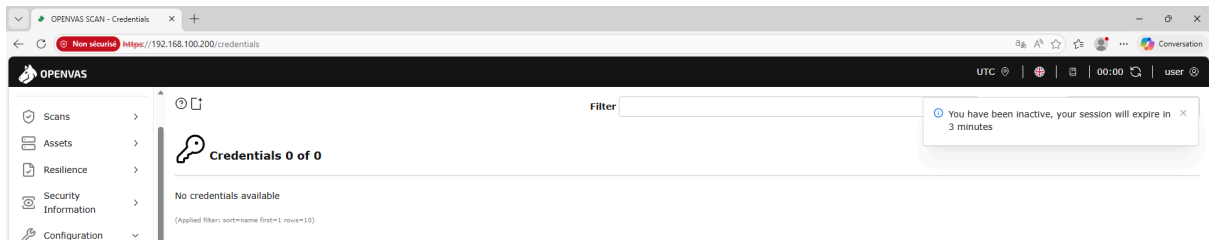
Affichage des systèmes d'exploitation détectés et des niveaux de criticité associés.



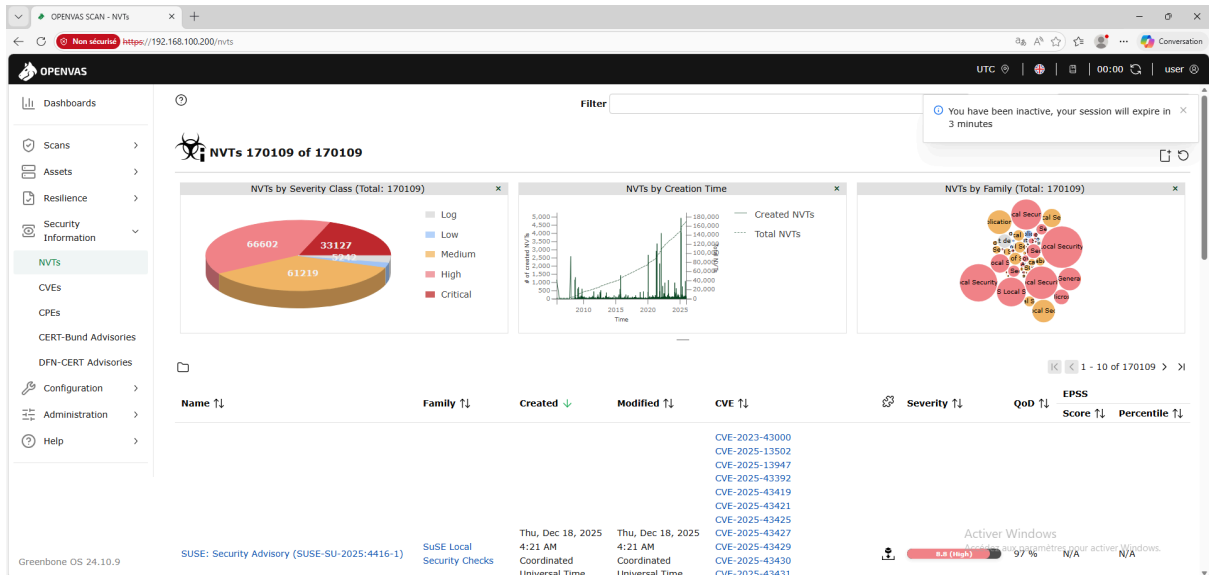
Consultation des différentes cibles configurées dans OpenVAS pour les scans de vulnérabilités.



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.

This screenshot provides a detailed view of vulnerability signatures. The table includes columns for the advisory name, family, creation/modification dates, CVE IDs, severity scores, and EPSS scores. For example, it lists 'SUSE: Security Advisory (SUSE-SU-2025:4416-1)' with CVEs like CVE-2025-43427 and CVE-2025-43429, and 'Fedora: Security Advisory (FEDORA-2025-ceeda3c40d)' with CVE-2025-9615. The severity scores range from 5.0 (Medium) to 9.8 (Critical).

Advisory Name	Family	Created	Modified	CVE	Severity	QoD	EPSS Score	Percentile
SUSE: Security Advisory (SUSE-SU-2025:4416-1)	SuSE Local Security Checks	Thu, Dec 18, 2025 4:21 AM	Thu, Dec 18, 2025 4:21 AM	CVE-2025-43427 CVE-2025-43429 CVE-2025-43430 CVE-2025-43431 CVE-2025-43432 CVE-2025-43434 CVE-2025-43440 CVE-2025-43443 CVE-2025-43458 CVE-2025-43480 CVE-2025-66287	9.8 (High)	97%	N/A	N/A
Fedora: Security Advisory (FEDORA-2025-ceeda3c40d)	Fedora Local Security Checks	Thu, Dec 18, 2025 4:17 AM	Thu, Dec 18, 2025 4:17 AM	CVE-2025-9615	5.0 (Medium)	97%	N/A	N/A
Fedora: Security Advisory (FEDORA-2025-c09b980696)	Fedora Local Security Checks	Thu, Dec 18, 2025 4:17 AM	Thu, Dec 18, 2025 4:17 AM	CVE-2025-58436 CVE-2025-61915	6.7 (Medium)	97%	N/A	N/A
Fedora: Security Advisory (FEDORA-2025-b8d9bd75d2)	Fedora Local Security Checks	Thu, Dec 18, 2025 4:17 AM	Thu, Dec 18, 2025 4:17 AM	CVE-2025-13372 CVE-2025-57833	5.0 (Medium)	97%	N/A	N/A
Fedora: Security Advisory (FEDORA-2025-b1379d950d)	Fedora Local Security Checks	Thu, Dec 18, 2025 4:17 AM	Thu, Dec 18, 2025 4:17 AM	CVE-2025-59681 CVE-2025-59682 CVE-2025-64459 CVE-2025-64460	9.8 (Critical)	97%	N/A	N/A
		Thu, Dec 18, 2025	Thu, Dec 18, 2025	CVE-2025-58185				

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

The screenshot shows the OpenVAS interface with a list of detected CVEs. The table includes columns for the CVE ID, description, severity, and associated advisories. The following table summarizes the visible data:

CVE ID	Description	Severity	Advisories
CVE-2025-58185, CVE-2025-58188, CVE-2025-58189, CVE-2025-61723	Fedora: Security Advisory (FEDORA-2025-bf07d21f3e)	3.8 (Medium)	Fedora Local Security Checks
CVE-2025-6176, CVE-2025-66471	Fedora: Security Advisory (FEDORA-2025-9e233a4e22)	7.5 (High)	Fedora Local Security Checks
CVE-2025-66459, CVE-2025-64460	Fedora: Security Advisory (FEDORA-2025-6e8c819299)	5.9 (Medium)	Fedora Local Security Checks
CVE-2025-13372, CVE-2025-57833, CVE-2025-59681, CVE-2025-59682, CVE-2025-64459, CVE-2025-64460	Fedora: Security Advisory (FEDORA-2025-45ee190318)	9.8 (Critical)	Fedora Local Security Checks
CVE-2025-13372, CVE-2025-57833, CVE-2025-59681, CVE-2025-59682, CVE-2025-64459, CVE-2025-64460	Fedora: Security Advisory (FEDORA-2025-24df3b072)	9.8 (Critical)	Fedora Local Security Checks

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

The screenshot shows a detailed view of CVEs in OpenVAS. It includes three charts and a table of specific CVEs.

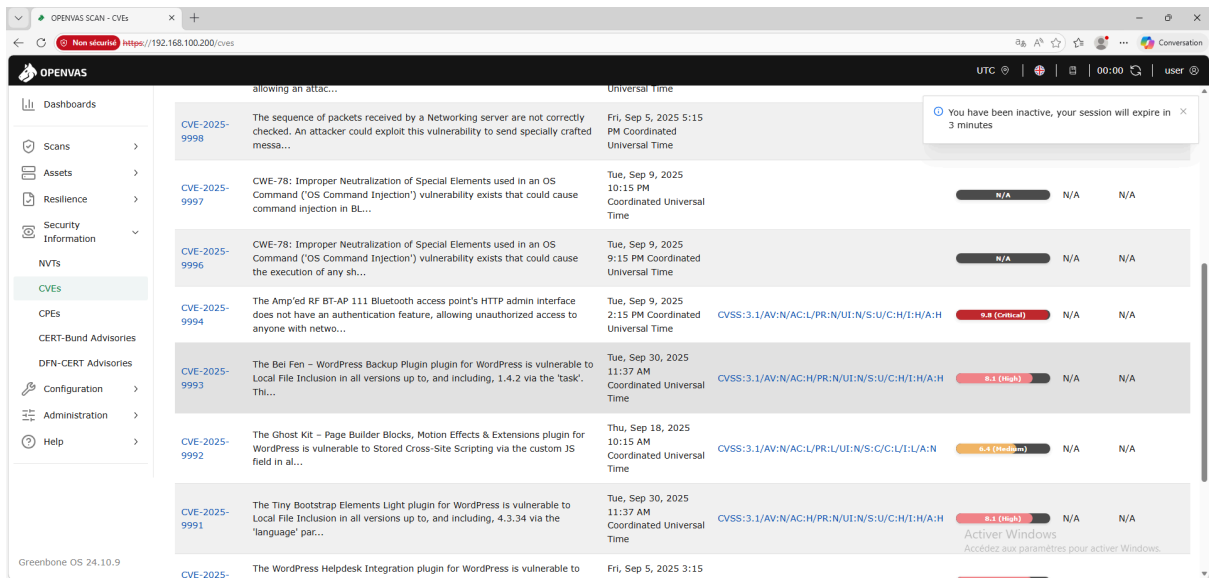
CVES 322960 of 322960

- CVES by Severity Class (Total: 322960):** A pie chart showing the distribution of CVEs by severity: N/A (108535), Log (43898), Low (10166), Medium (20483), High (139858), and Critical (20483).
- CVES by Creation Time:** A line graph showing the number of CVEs created over time from 1990 to 2020.
- CVES by CVSS (Total: 322960):** A bar chart showing the number of CVEs for each CVSS score from 0 to 10.

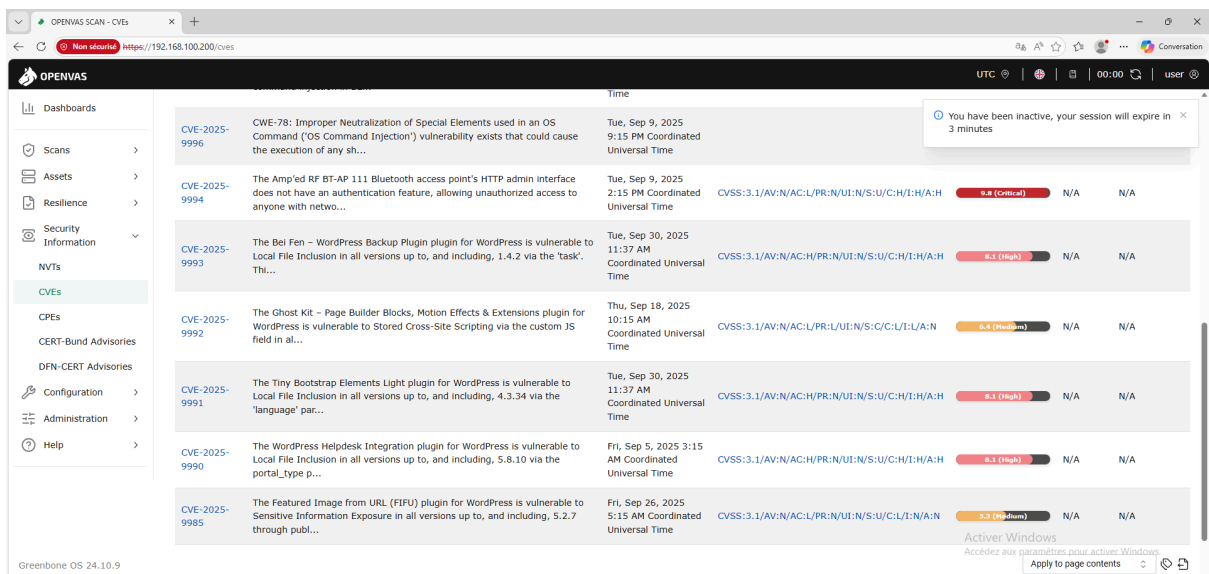
The table below shows the details of three CVEs:

Name	Description	Published	CVSS Base Vector	Severity	EPSS Score	Percentile
CVE-2025-9999	Some payload elements of the messages sent between two stations in a networking architecture are not properly checked on the receiving station allowing an attac...	Fri, Sep 5, 2025 5:15 PM Coordinated Universal Time		N/A	N/A	N/A
CVE-2025-9998	The sequence of packets received by a Networking server are not correctly checked. An attacker could exploit this vulnerability to send specially crafted messa...	Fri, Sep 5, 2025 5:15 PM Coordinated Universal Time		N/A	N/A	N/A
CVE-2025-9997	CWE-78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection") vulnerability exists that could cause	Tue, Sep 9, 2025 10:15 PM Coordinated Universal Time		N/A	N/A	N/A

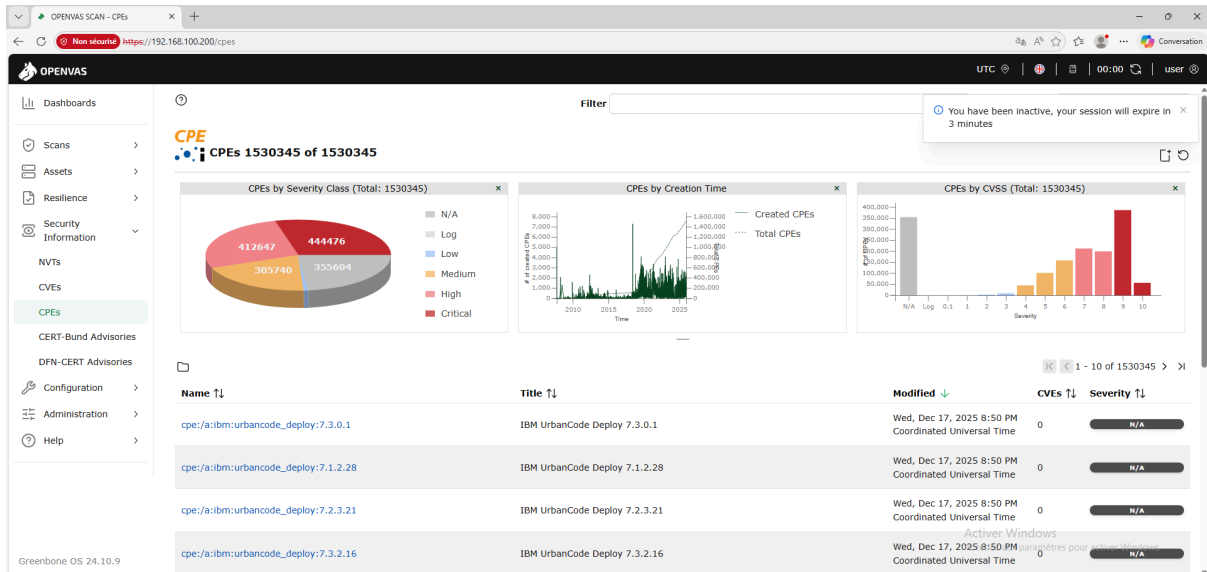
Affichage des logiciels et composants détectés via les identifiants CPE pendant le scan.



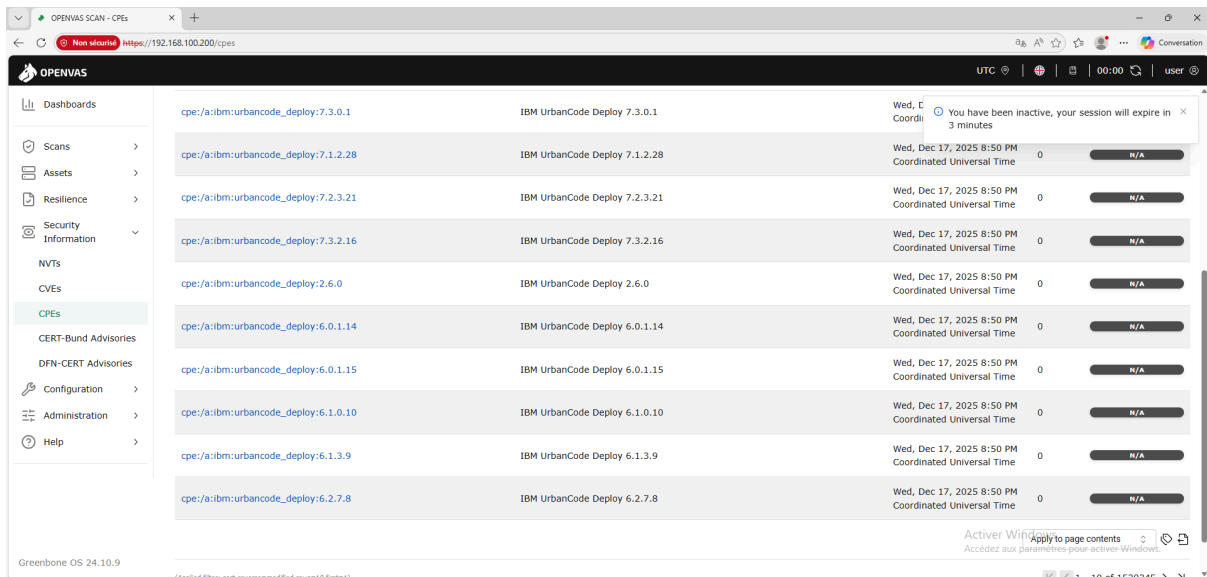
Analyse détaillée des applications détectées et des versions logicielles présentes sur la machine cible.



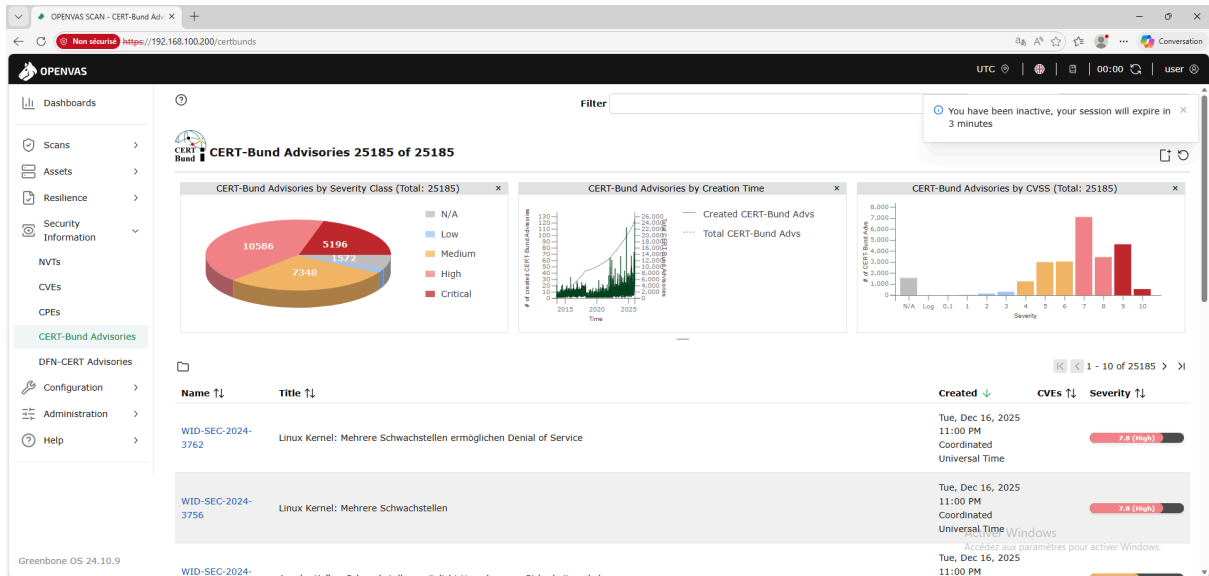
Consultation des avis CERT-Bund liés aux vulnérabilités détectées sur Damn Vulnerable Linux.



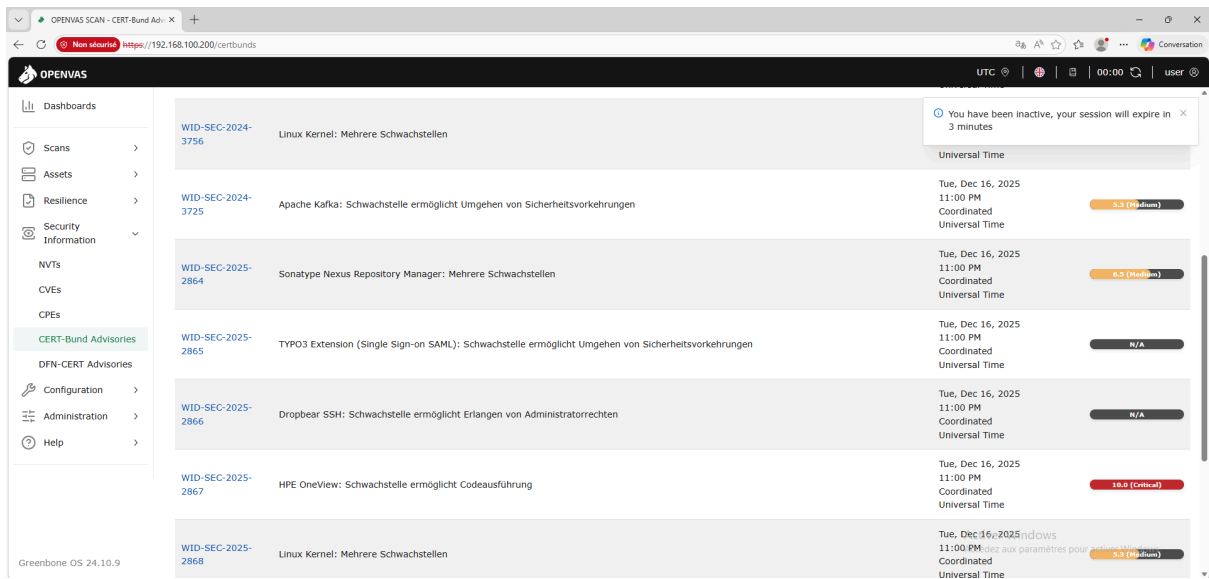
Analyse détaillée des alertes CERT-Bund et des niveaux de sévérité associés aux failles détectées.



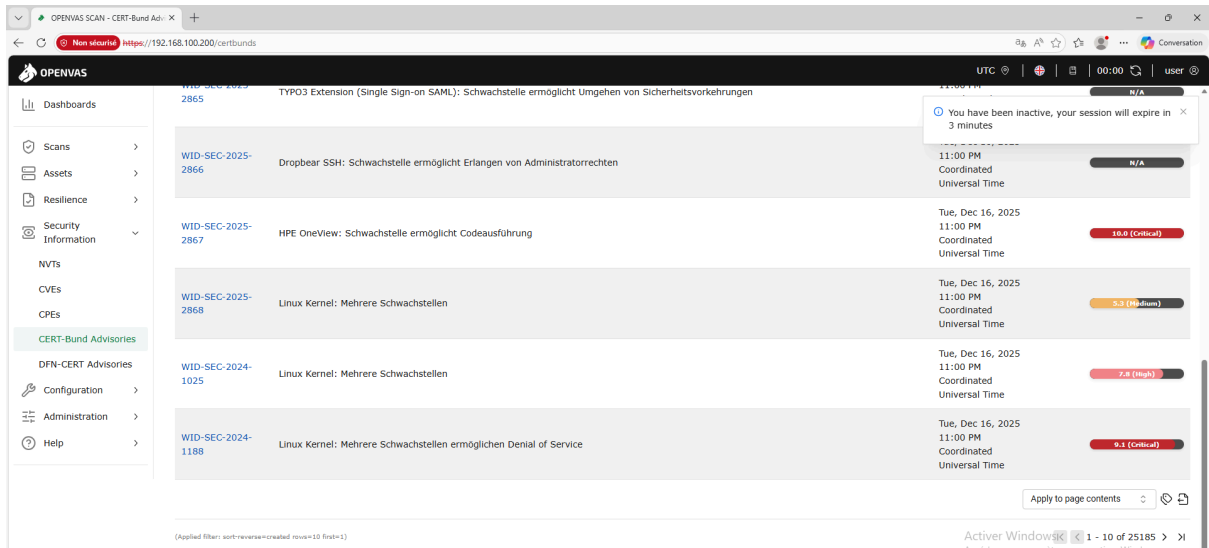
Consultation des avis DFN-CERT concernant les vulnérabilités identifiées lors du scan.



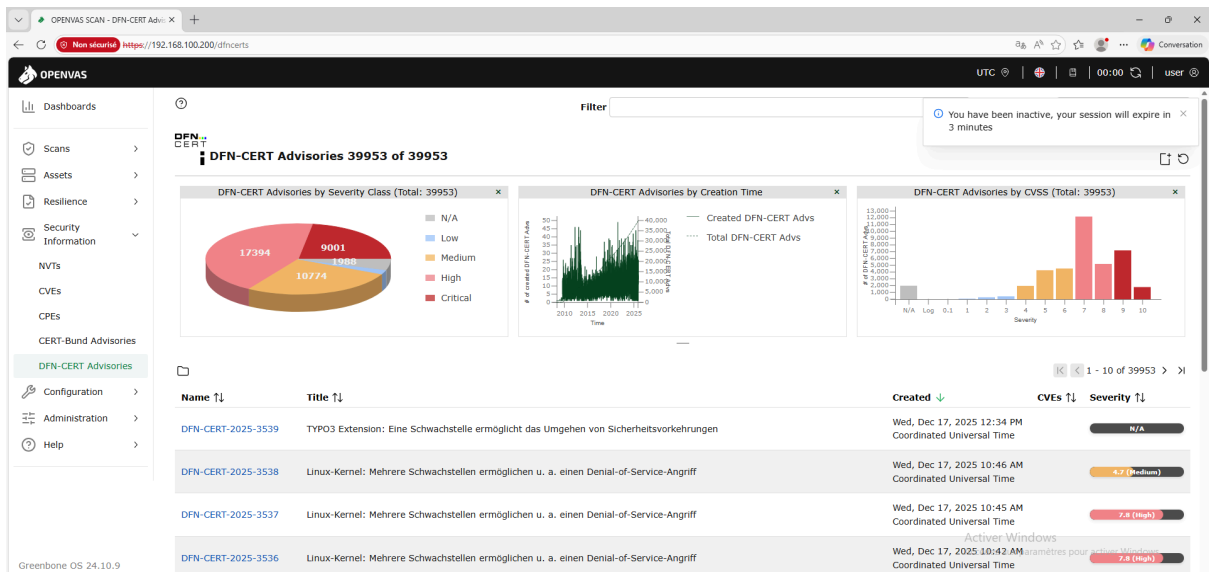
Analyse détaillée des alertes DFN-CERT et des recommandations de sécurité associées.



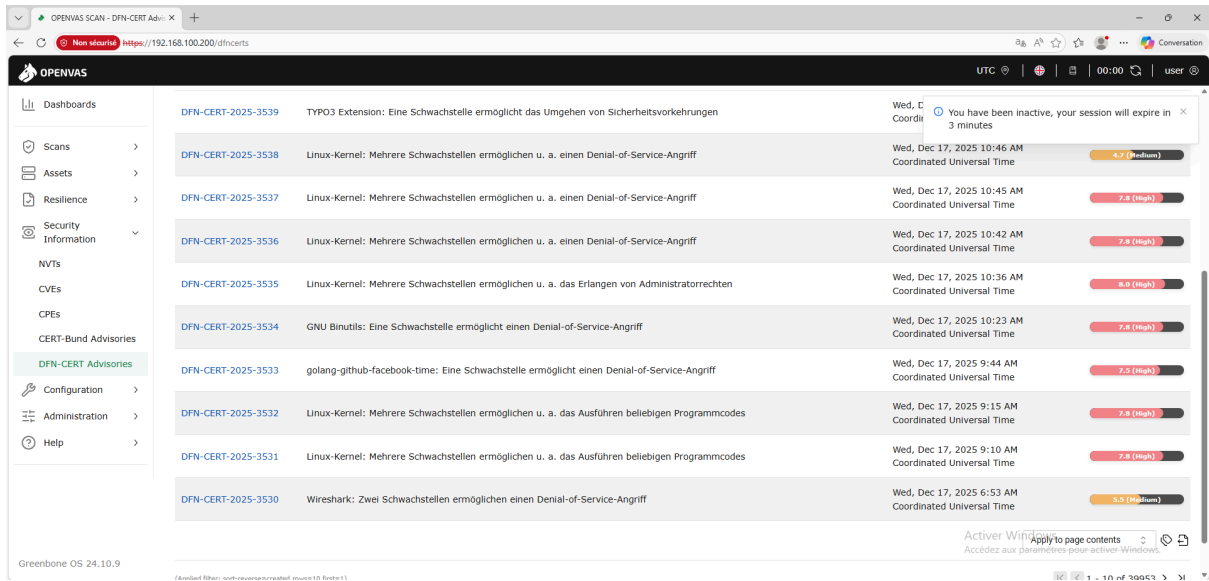
Consultation des politiques de conformité et des modèles d'audit de sécurité disponibles dans OpenVAS.



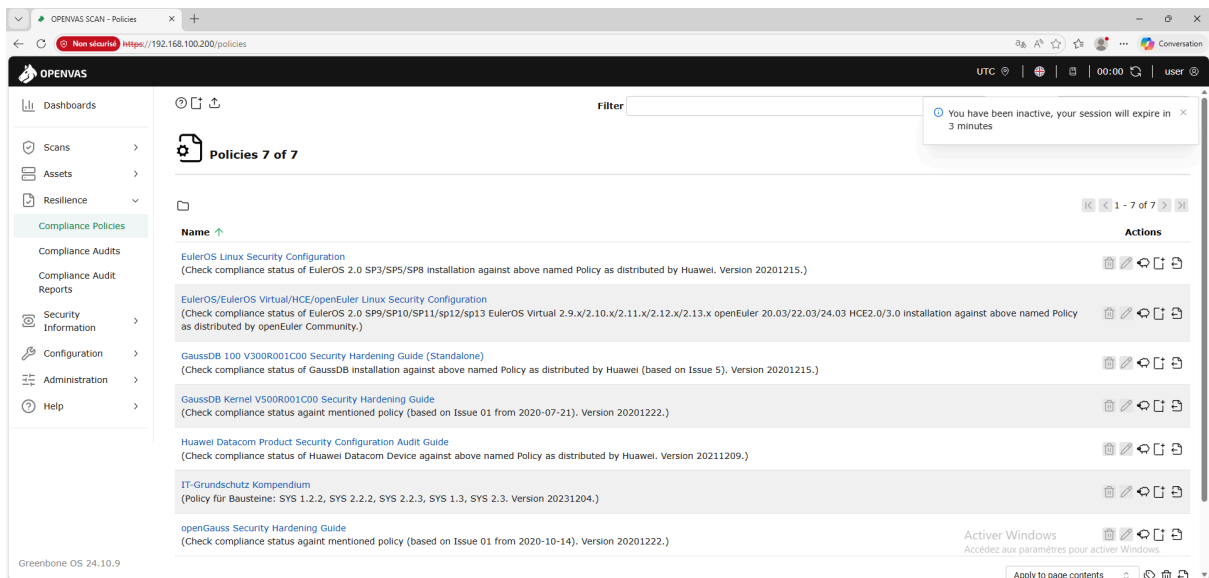
Affichage de la liste des vulnérabilités détectées sur Damn Vulnerable Linux avec leur criticité.



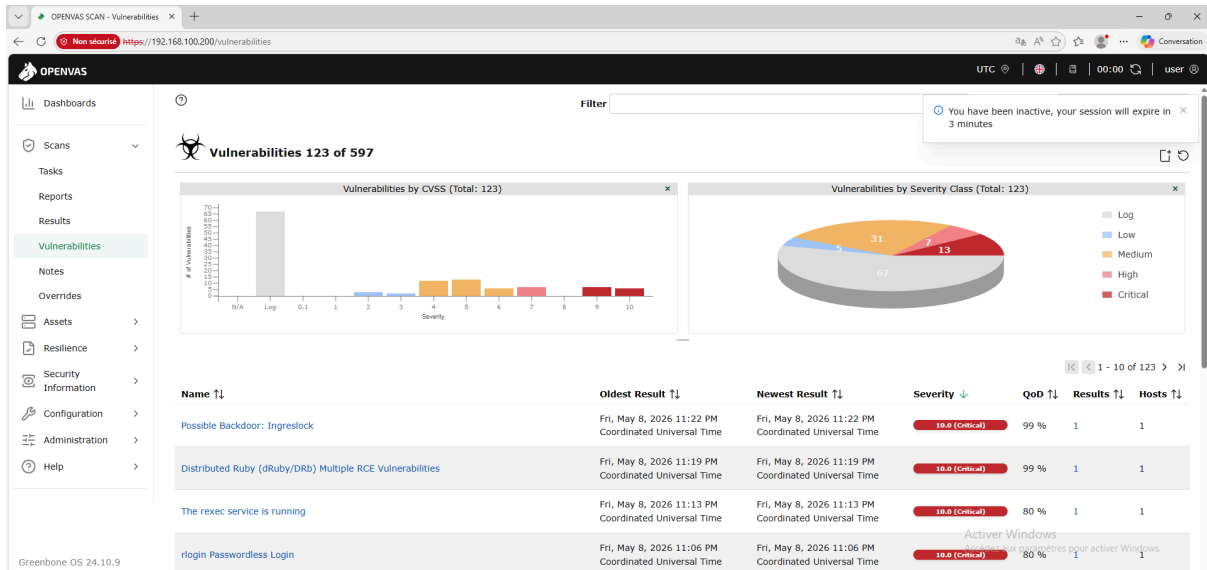
Analyse détaillée des principales failles de sécurité identifiées pendant le scan OpenVAS.



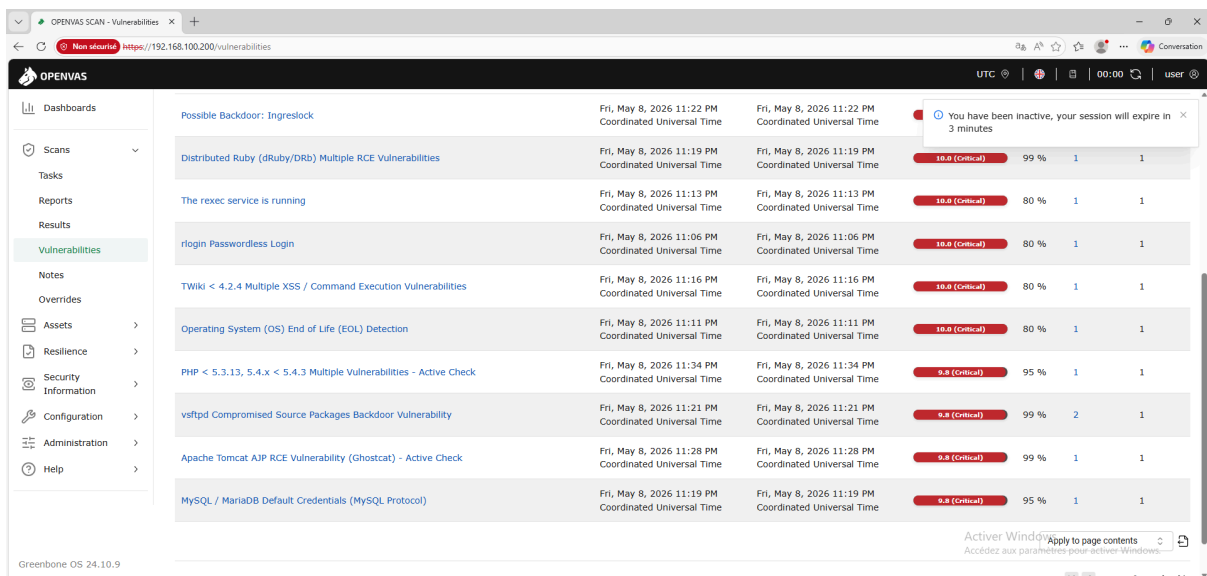
Consultation des politiques de conformité et des modèles d’audit de sécurité disponibles dans OpenVAS.



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.