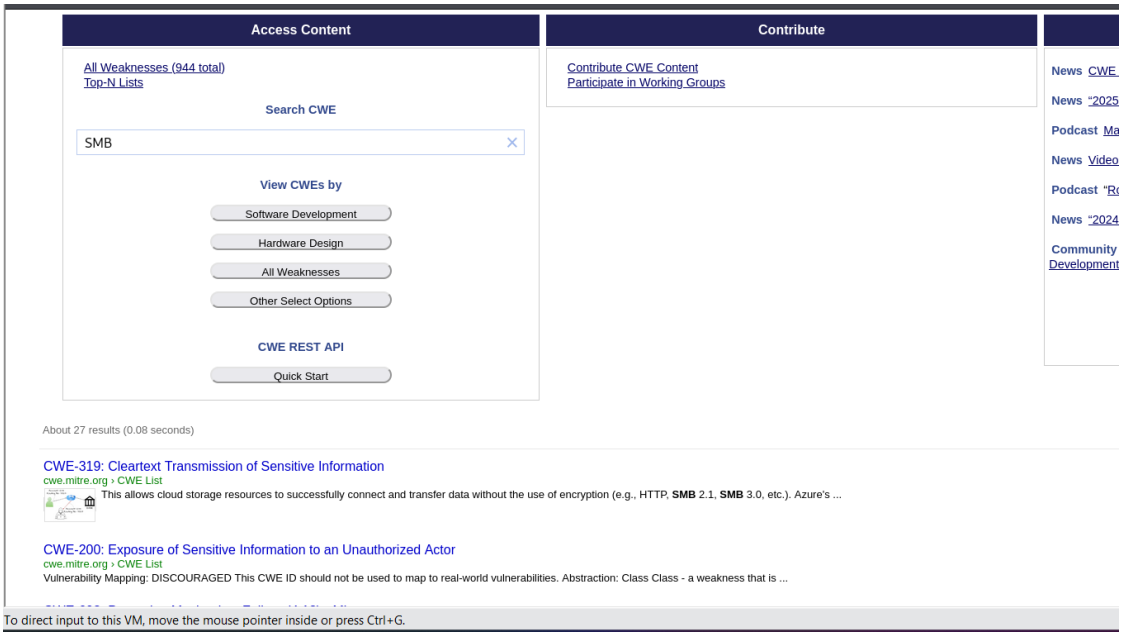
TP : Recherche et analyse de vulnérabilités

Issa MENTA

Partie 1

1.1 Recherche de SMB dans la base CWE – Vulnérabilités SMB



1. Recherche “SMB” dans CWE Mitre

En cherchant “SMB” sur le site CWE Mitre, on trouve plusieurs faiblesses associées au protocole Server Message Block (SMB).

Vulnérabilités courantes liées à SMB

Voici les plus fréquentes que j’ai trouvé:

- CWE-20 – Improper Input Validation
  (exploitation via paquets SMB malformés)
- CWE-200 – Exposure of Sensitive Information
  (ex : fuite d’infos via SMBv1)
- CWE-287 – Improper Authentication
  (authentification faible ou désactivée)

- CWE-522 – Insufficiently Protected Credentials
  (mots de passe envoyés en clair)
- CWE-611 – Improper Restriction of XML External Entity (si utilisé)
- CWE-693 – Protection Mechanism Failure
  (mécanismes de sécurité insuffisants : SMBv1, NTLMv1)

Les exemple de vulnérabilité sélectionnée : CWE-287 – Improper Authentication

Description courte :
Le service SMB n'applique pas correctement l'authentification, permettant à un attaquant d'accéder à des ressources sans fournir des identifiants valides.

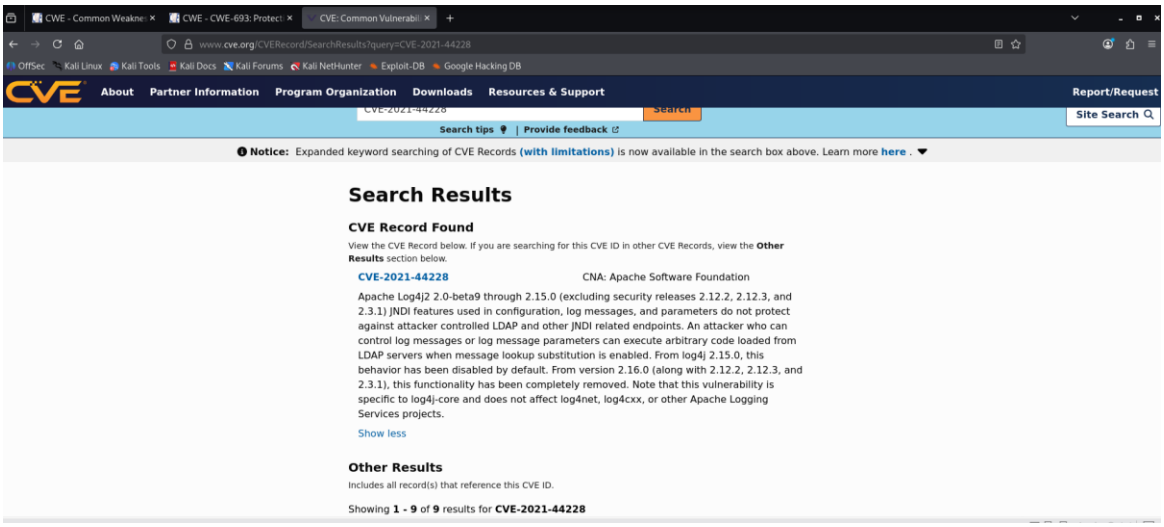
Conséquences :

- Accès non autorisé
- Exfiltration de données
- Mouvement latéral

Exemples d'exploitation :

- SMB avec authentification nulle activée
- Partages accessibles à "Everyone"
- Weak NTLM authentication

1.2 Recherche dans la base CVE – Exemple : CVE-2021-44228



Quelques détails depuis CVE Mitre

- CVE ID : CVE-2021-44228
- Produit affecté : Apache Log4j2 versions 2.0-beta9 à 2.15.0
- Type de vulnérabilité : Remote Code Execution (RCE) via JNDI
- Cause :
  Log4j ne protège pas correctement l'utilisation de JNDI dans la configuration, les messages et les paramètres.
- Exploit :
  Un attaquant qui contrôle une donnée loguée peut injecter une chaîne du type :
- → Cela charge du code depuis un serveur LDAP malveillant → exécution de code à distance.
- **Corrections :**
  - 2.15.0 : JNDI désactivé par défaut
  - 2.16.0+ : fonctionnalité supprimée
  - Versions maintenues corrigées : 2.12.2, 2.12.3, 2.3.1

Comparaison avec NVD (NIST)

Sur NVD, les informations sont similaires mais plus détaillées :

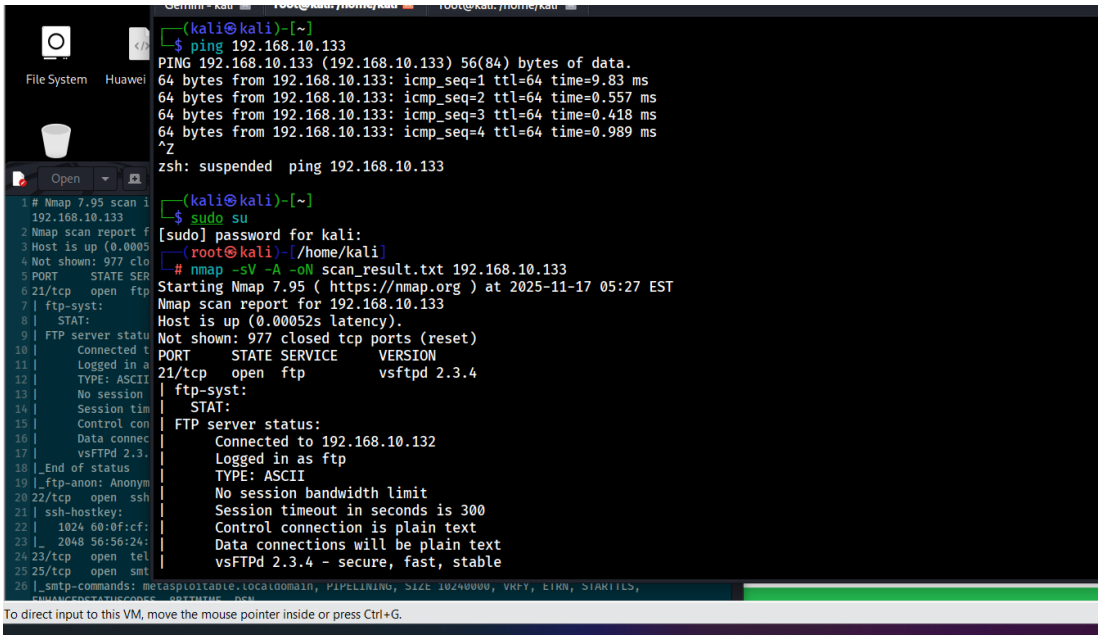
- Score CVSS v3.1 : 10.0 (critique)
- Impact :
  - RCE complète
  - Confidentialité/Intégrité/Disponibilité : compromises totalement
- Vecteur d'attaque :
  - Network
  - Complexité faible
  - Pas d'authentification nécessaire

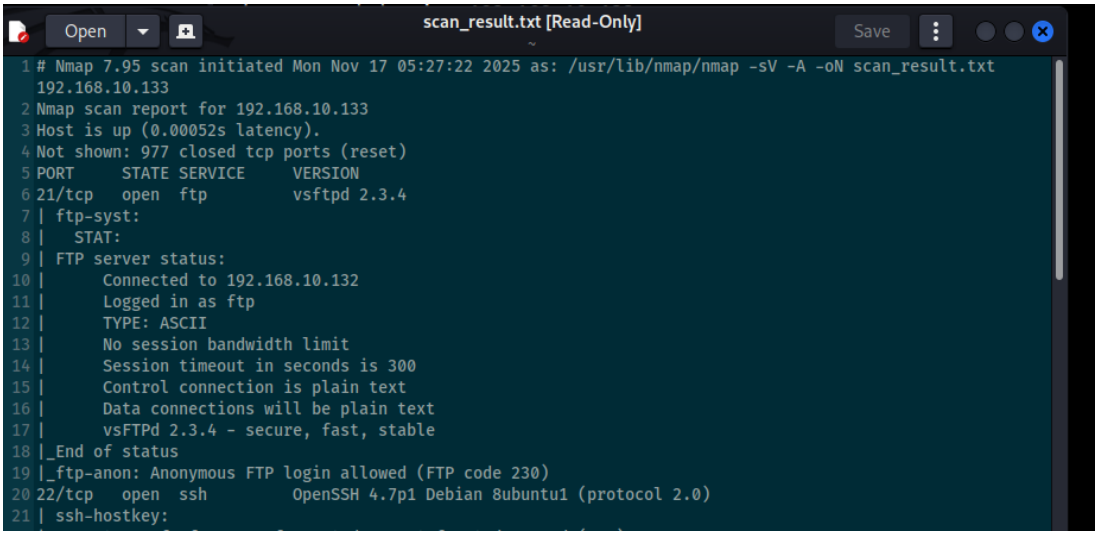
NVD ajoute :

- Des informations sur les configurations affectées
- Des références vers les exploits publics
- Des patchs et mesures d'atténuation
- Le score vectoriel complet :
  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

PARTIE 2 – SCANS NMAP + NIKTO + RECHERCHE EXPLOITS

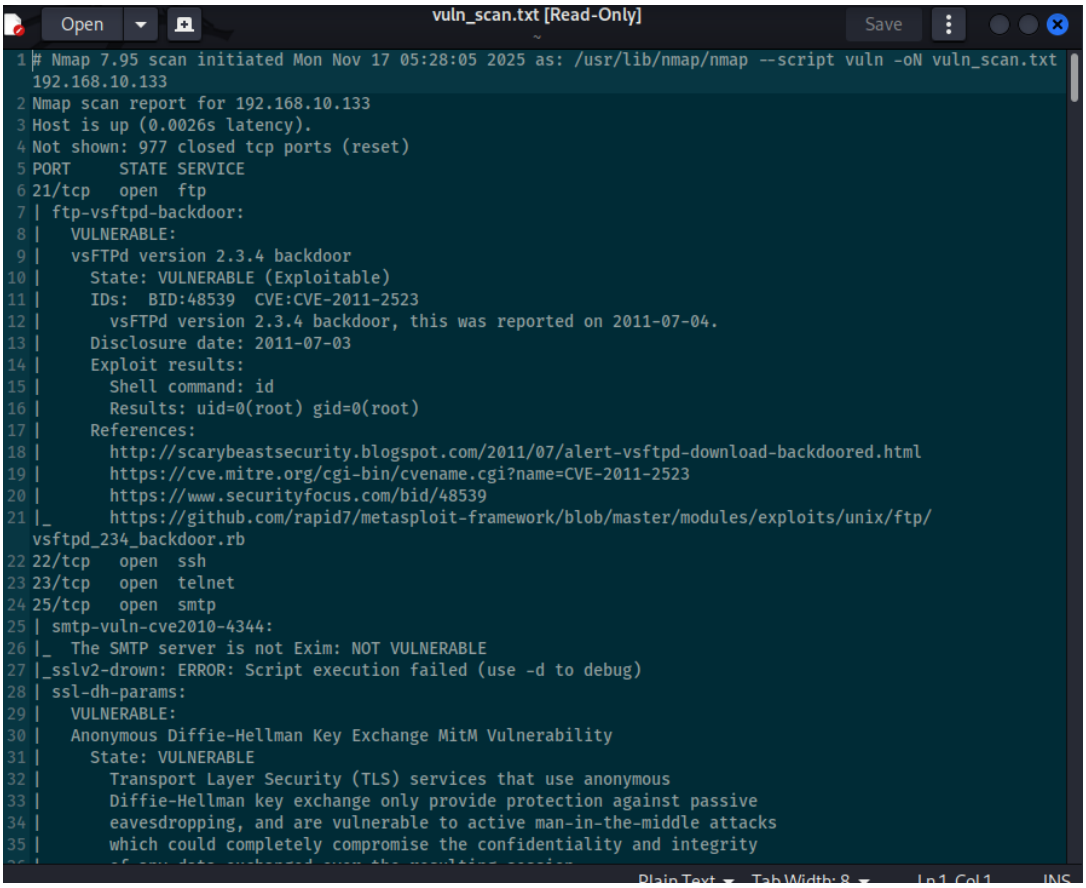
Étape 1: Scan du réseau avec Nmap





1- Analyse des résultats et des services ouverts

```
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdo
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
```



Étape 2 : Détection automatique de vulnérabilités Nmap

2- Voici les vulnérabilités Nikto + leurs CVE typiques :

Vulnérabilité Nikto	Description	CVE associé
Apache 2.2.8 obsolète	Version non maintenue pouvant contenir de multiples failles	**CVE-2011-3192**, **CVE-2010-1452**, etc.
PHP 5.2.4 exposé	Version vulnérable à RCE et LFI	**CVE-2007-4887**, **CVE-2007-3996**
phpinfo() accessible	Fuite d'infos sensibles	**CVE-2007-0405**
Directory listing activé	Exposition de fichiers	Non spécifique (faiblesse configuration)
TRACE method activé	Vulnérable à XST	**CVE-2004-2763**
PHP Easter Eggs (PHPE9568F36...)	Fuite d'infos PHP	**OSVDB-12184**
phpMyAdmin accessible publiquement	Fuite d'infos, brute force	**CVE-2009-1151**, **CVE-2012-5159**

Exemples d'exploits trouvés :

CVE	Exploit disponible	Type
CVE-2011-3192	Oui	DoS Apache
CVE-2007-4887	Oui	RCE PHP
CVE-2009-1151	Oui	Auth bypass phpMyAdmin

3. Niveau de criticité (CVSS)

CVE	Score CVSS	Criticité
CVE-2011-3192	7.8	High
CVE-2007-4887	10.0	Critical
CVE-2009-1151	7.5	High
CVE-2004-2763	4.3	Medium

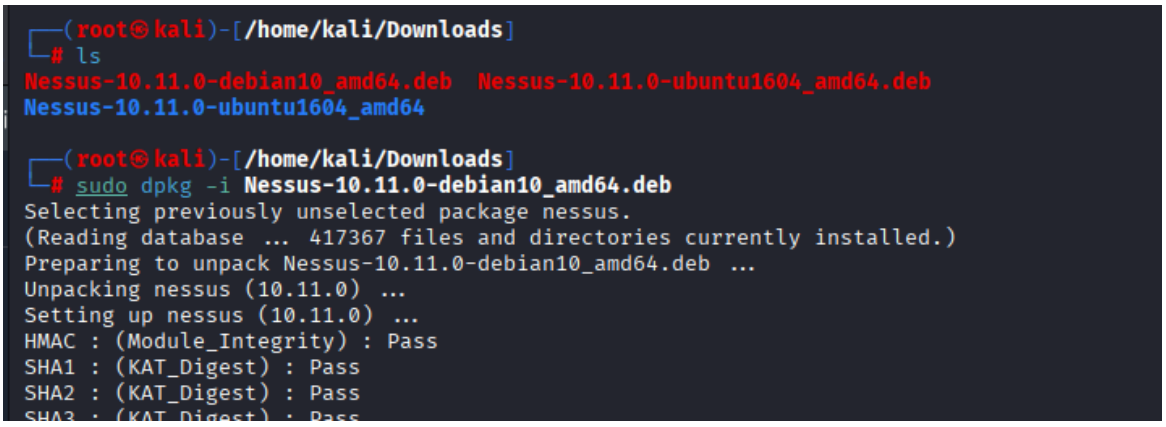
4. Mesures correctives

- Mettre à jour **Apache** (>= 2.4).
- Mettre à jour **PHP** (>= 8.x).
- Désactiver la méthode **TRACE** :
- Supprimer **phpinfo.php**.
- Restreindre l'accès à **phpMyAdmin** (pare-feu + authentification).
- Désactiver **directory listing** (Options -Indexes).
- Désactiver **MultiViews** pour éviter les bruteforce de fichiers.
- Ajouter des en-têtes de sécurité (X-Frame-Options, X-Content-Type-Options).

PARTIE 3 – NESSUS

1- **Téléchargement de Nessus pour Kali**

2- **Installation de Nessus**



Une fois installer on va démarrer Nessus.

3- Démarrage de Nessus

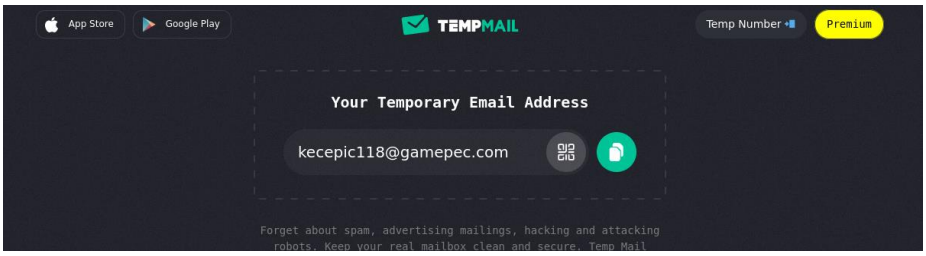
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo systemctl start nessusd

┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disab>
     Active: active (running) since Sat 2025-11-22 12:40:06 EST; 25s ago
 Invocation: ed6bb740fa804606ba527340d269254f
   Main PID: 32940 (nessus-service)
      Tasks: 16 (limit: 2197)
     Memory: 171.2M (peak: 200.2M)
        CPU: 25.147s
     CGroup: /system.slice/nessusd.service
             ├─32940 /opt/nessus/sbin/nessus-service -q
             └─32949 nessusd -q
```

2.2 Création d'un Scan avec Nessus

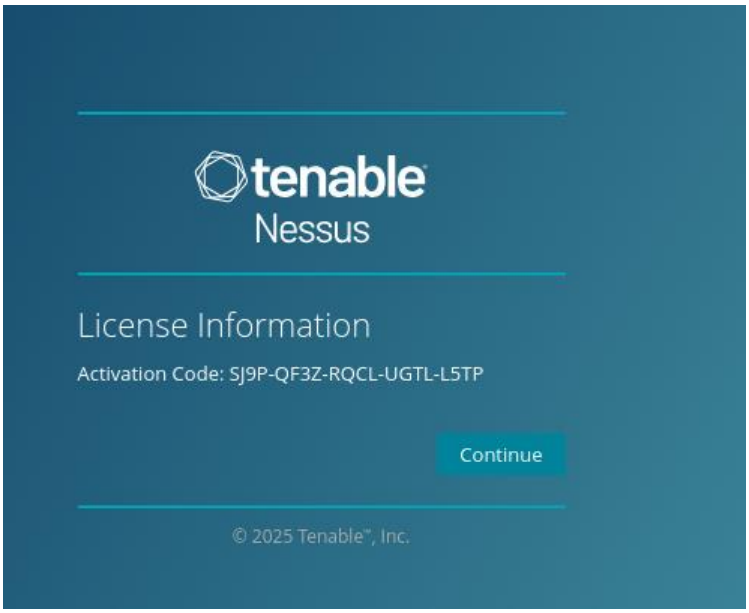
2.1. Se connecter à Nessus.

⇨ Ici, on va récupérer une adresse email professionnel sur le site temp email :

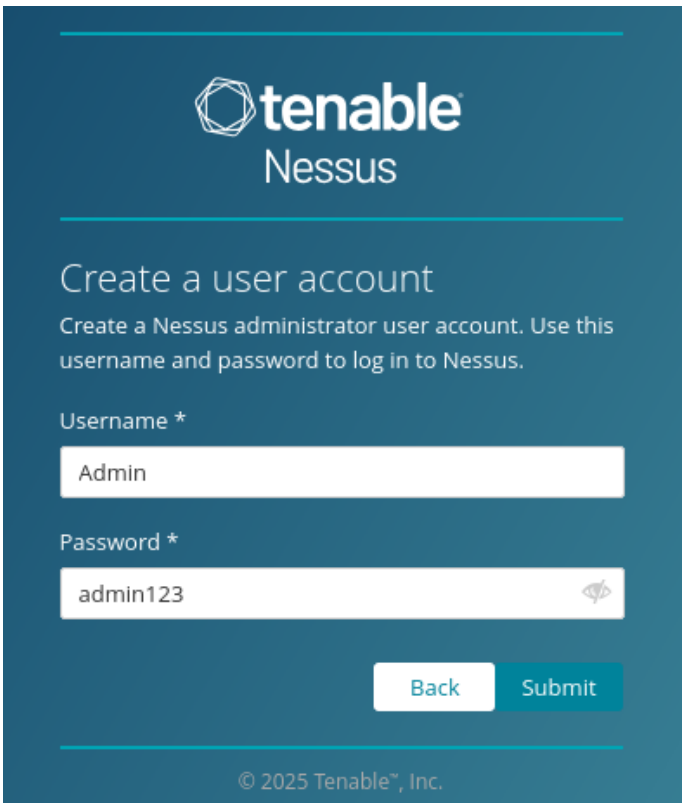


Tel est l'adresse email qu'on va utiliser pour se connecter.

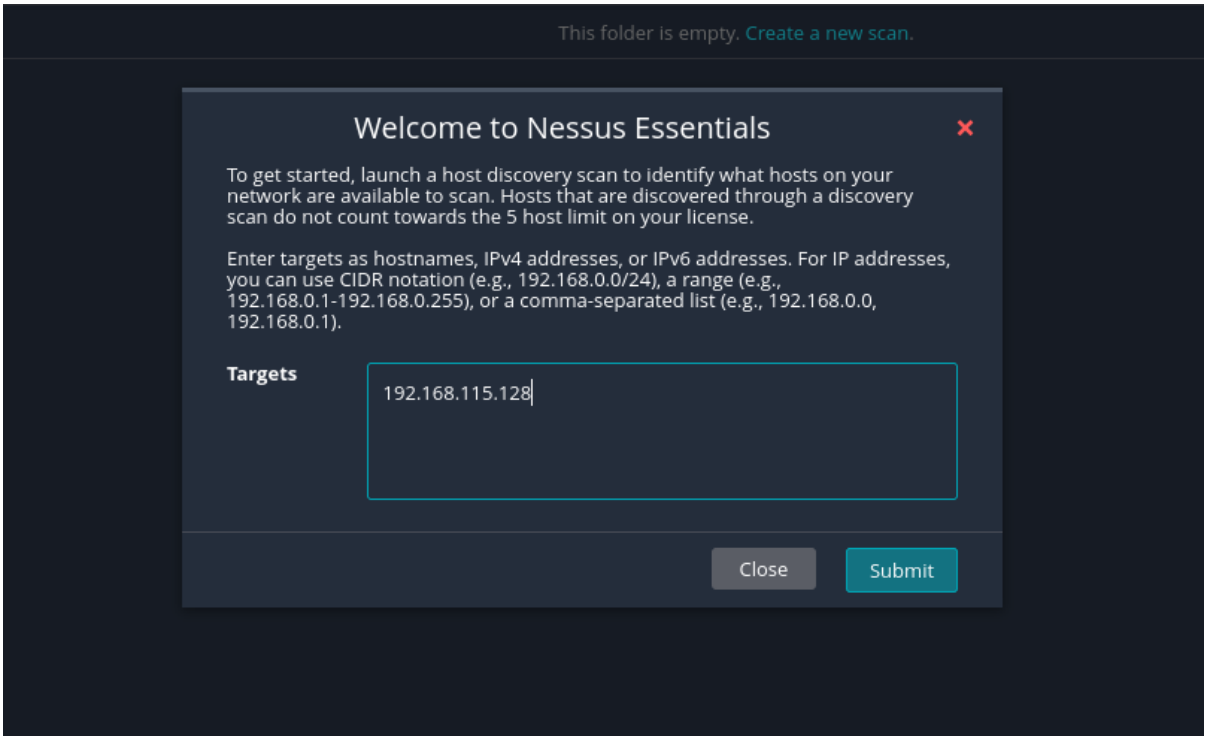
Ici, on voit notre code d'activation



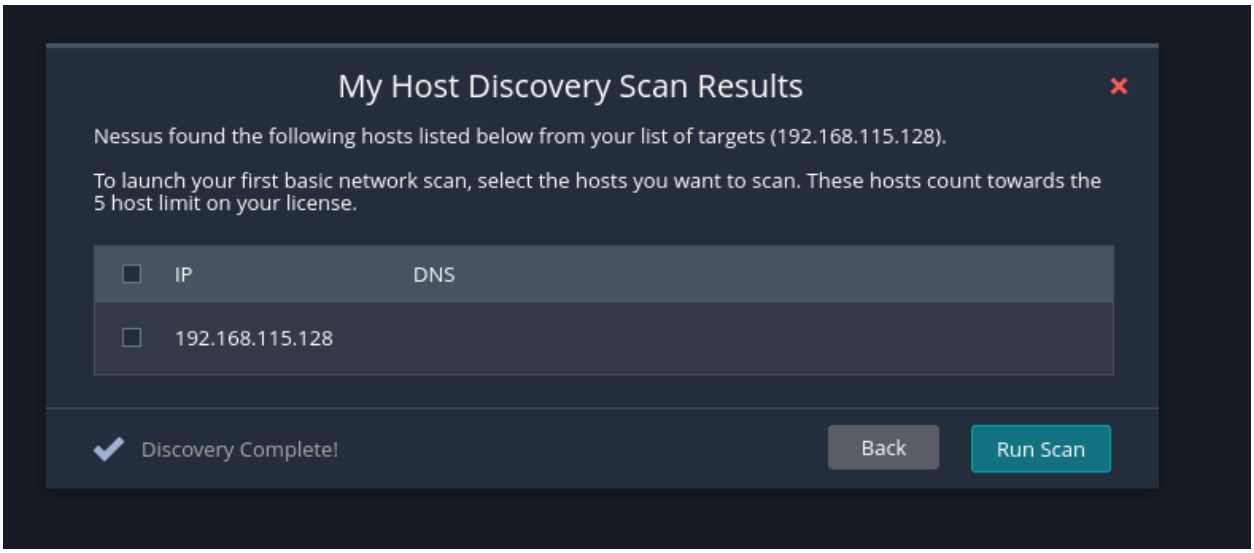
- ⇨ Ensuite, on donne les identifiantes pour se connecter Nessus :



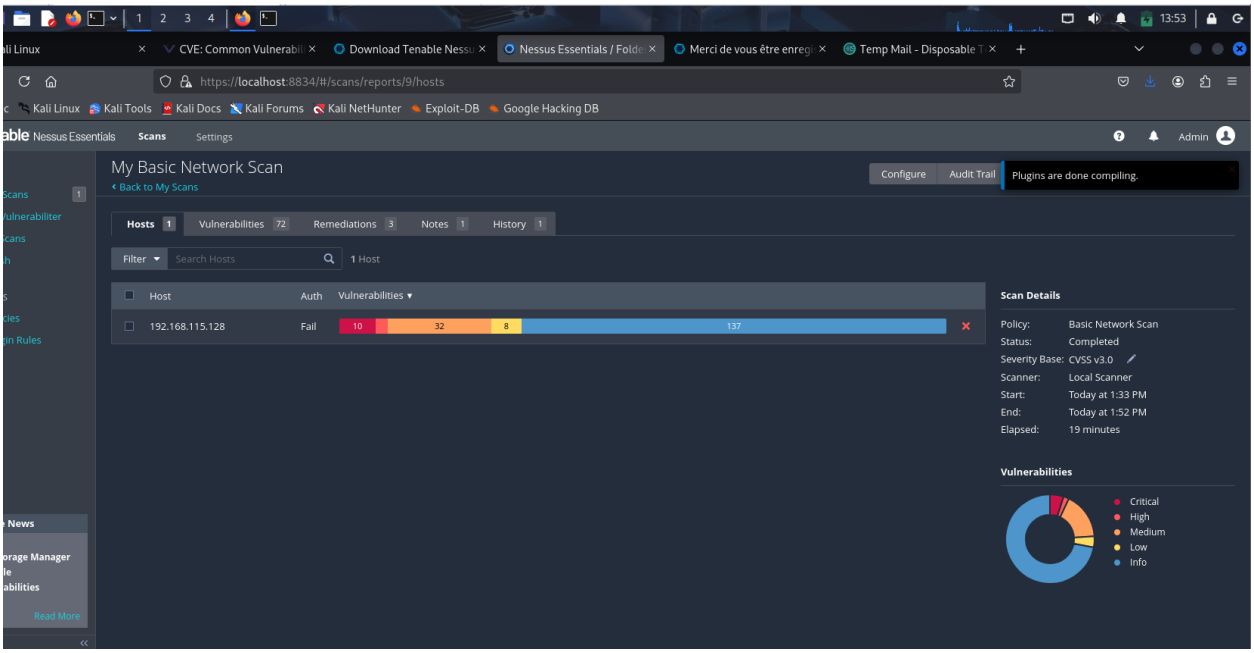
2.2. Créer un nouveau scan :



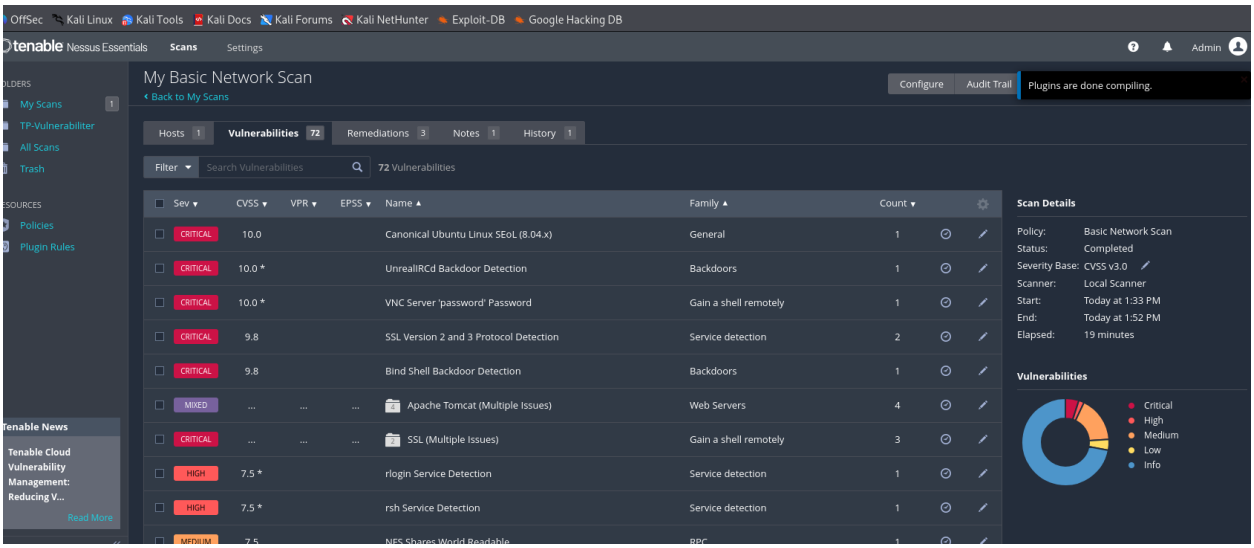
On sélection l'IP qu'on doit scanner et puis on run scan :



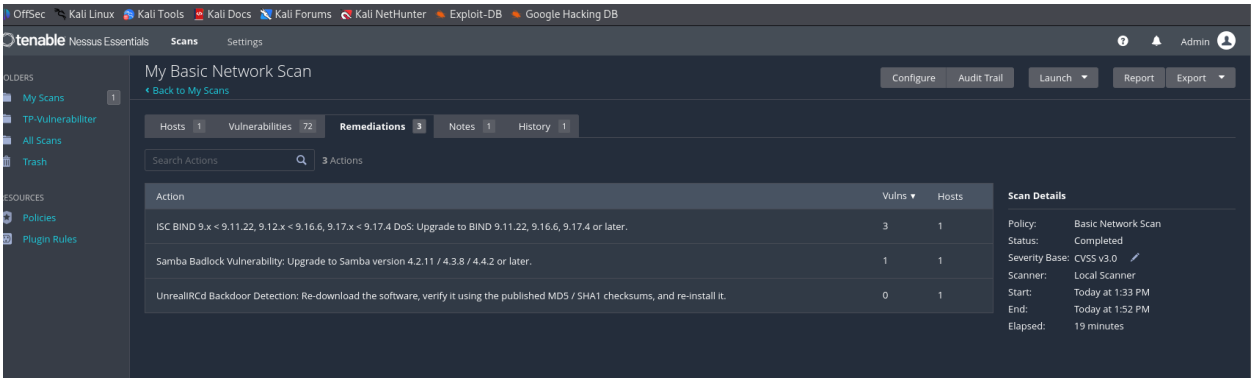
2.3 Analyse des Résultats



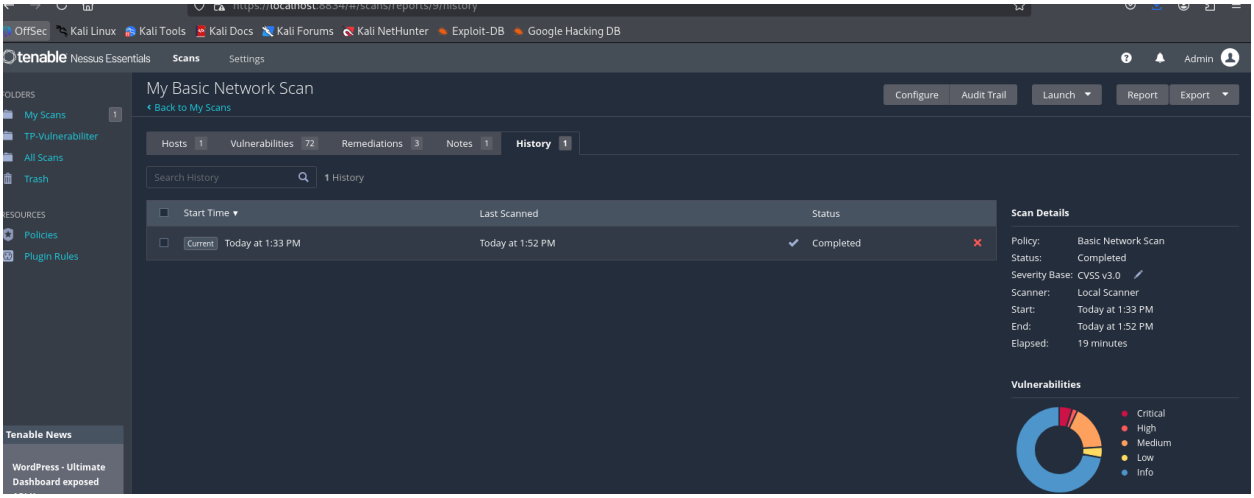
La page qui nous montre les vulnérabilités :



⇨ Remédiations :



⇨ History :



1. **Une fois le scan terminé, ouvrez Scans, Complètez et commentez les résultats.**
   La machine analysée présente un grand nombre de vulnérabilités, dont plusieurs critiques, indiquant qu'il s'agit probablement d'un système volontairement vulnérable (comme Metasploitable). De nombreux services sont exposés et reposent sur des versions anciennes présentant des failles connues.
2. **Analyse des résultats :**
   a. Vulnérabilités détectées
   Le scan révèle dix vulnérabilités critiques susceptibles de permettre une exécution de code à distance (RCE) ou une compromission complète du système.
   Trente-deux vulnérabilités de niveau élevé concernent principalement des services obsolètes comportant des failles connues.
   Huit vulnérabilités de niveau moyen relèvent surtout de problèmes de configuration et de protocoles insuffisamment sécurisés.

b. Recommandations proposées

Nessus recommande avant tout la mise à jour des logiciels obsolètes, la désactivation des services non indispensables, l'application des correctifs de sécurité et le renforcement des protocoles de chiffrement.

Pour les vulnérabilités critiques, une mise à jour immédiate des composants concernés (Samba, FTP, Apache, SSH, etc.) est préconisée.

Conclusion :

Ce travail pratique a permis d'apprendre à identifier des vulnérabilités connues et à analyser une machine à l'aide d'outils tels que Nmap, Nikto et Nessus. Les résultats ont mis en évidence de nombreuses failles, dont certaines particulièrement graves. Cette analyse souligne l'importance de maintenir les systèmes à jour, d'appliquer les correctifs nécessaires et de sécuriser les ports ouverts.

En définitive, ce TP démontre que l'analyse de vulnérabilités constitue une étape essentielle pour prévenir les attaques et garantir la sécurité d'un système.