

Rapport d'Assessment de Vulnérabilités

Projet personnel

Réalisé par :

Nada Maach

Table des matières

Introduction personnelle et portée	1
Sommaire d'exécution	2
Conditions de test	2
Résultats globaux	2
Résultats globaux et analyse	3
Failles cryptographiques	3
Composants et systèmes obsolètes	3
Contrôles d'accès et authentification faibles	3
Injection et exécution arbitraire	3
Recommandations prioritaires	4
Plan d'action	4
Contexte et méthodologie	5
Analyse de risque globale	5
Annexe technique	5
Conclusion	19

Introduction personnelle et portée

Ce rapport d'assessment de vulnérabilités constitue un projet personnel permettant d'appliquer et de développer mes compétences en cybersécurité. Le framework suivi pour la forme du rapport est celui fourni par EC-Council, garantissant un format professionnel reconnu dans l'industrie. Ce projet m'a permis de travailler sur les points suivants :

- Utilisation des outils d'analyse de vulnérabilités (Nessus, Nmap) pour identifier et cartographier les faiblesses techniques.
- Application des étapes d'analyse de vulnérabilités, de la découverte des services à l'évaluation des risques.
- Analyse et rédaction d'un rapport complet d'assessment de vulnérabilités.
- Lecture et synthèse des résultats obtenus pour produire un résumé clair et exploitable.
- Utilisation d'API vulnérabilité pour récupérer les identifiants CVE et intégrer ces informations dans un script Python, permettant de combiner et d'exploiter les résultats Nmap pour une meilleure compréhension.
- Approfondissement des connaissances sur les types de vulnérabilités et les logiciels vulnérables, notamment la gestion des certificats SSL/TLS. Une formation complémentaire sur ce sujet a été suivie sur la plateforme Addison.

Limitations et contraintes du projet :

- Les enjeux métier de l'entreprise n'ont pas été pris en compte.
- Les liens vers les correctifs, mises à jour et exigences réglementaires n'ont pas été inclus.
- En raison de contraintes liées à la version de Nessus utilisée, l'évaluation a été réalisée avec CVSS v2.0, bien que les versions CVSS v3.0 et v4.0 soient disponibles. Dans un contexte professionnel, ce choix serait inacceptable, mais il est suffisant pour un projet pédagogique.

1. Sommaire d'exécution

Portée et objectifs de l'évaluation

L'objectif de cet *assessment* de vulnérabilités est d'évaluer l'état de sécurité d'une machine Linux. La portée de l'analyse est strictement limitée aux vulnérabilités techniques détectées sur la machine scannée.

Les éléments suivants ne sont pas couverts dans cette phase :

- processus métiers.
- évaluation de l'impact organisationnel (métriques environnementaux du CVSS).
- conformité réglementaire et normative.

Conditions de test

Les tests ont été réalisés sur une machine Linux Metasploitable, volontairement vulnérable, accessible à l'adresse IP 192.168.56.129. L'audit a été mené depuis une machine Kali Linux située sur le même réseau.

- **Nmap** : utilisé pour la découverte d'hôtes, l'identification des services, la détection de l'OS et le ping scan.
- **Nessus** : utilisé pour l'analyse approfondie des vulnérabilités et la priorisation des résultats.

Résumé des résultats

- 10 vulnérabilités critiques
- 5 vulnérabilités de sévérité élevée
- 24 vulnérabilités de sévérité moyenne
- 8 vulnérabilités de sévérité basse



FIGURE 1 – Répartition des vulnérabilités par niveau de sévérité

2. Assessment overview

L'audit a mis en évidence plusieurs vulnérabilités critiques, dont la majorité correspond aux catégories de l'OWASP Top 10.

Failles cryptographiques

- Génération de clés prévisibles
- Protocoles obsolètes et vulnérables (SSLv2/SSLv3, POODLE, attaques de downgrade)
- **Risque** : compromission de la confidentialité des communications

Composants et systèmes obsolètes

- OS en fin de vie et services non maintenus
- **Risque** : exposition à des attaques opportunistes exploitant des CVE connues

Contrôles d'accès et authentification faibles

- Authentification triviale et brute force possible
- Backdoor permettant l'exécution de commandes à distance
- **Risque** : compromission complète du système

Injection et exécution arbitraire

- Exploitation via AJP permettant lecture/écriture de fichiers arbitraires
- **Risque** : compromission du serveur (Injection – OWASP Top 10)

En complément, des vulnérabilités récurrentes dans la gestion des certificats SSL/TLS ont été détectées :

- certificats auto-signés, expirés ou mal configurés,
- noms d'hôtes incorrects.

Ces faiblesses exposent le système à des risques transversaux :

- attaques Man-in-the-Middle et usurpation de serveur,

- compromission de la confidentialité et intégrité des échanges,
- perte de confiance des utilisateurs.

En résumé : l'environnement testé souffre de vulnérabilités critiques combinant faiblesses cryptographiques, composants obsolètes et déficiences dans l'authentification. Cela place le système dans une posture à haut risque, nécessitant des mesures correctives rapides.

3. Recommandations prioritaires

Les mesures de remédiation doivent cibler en priorité les vulnérabilités critiques :

- Mettre à jour la configuration AJP pour exiger une authentification et migrer Apache Tomcat vers une version supportée.
- Migrer Ubuntu Linux vers une version supportée par Canonical.
- Régénérer tout le matériel cryptographique (clés SSH, SSL, OpenVPN).
- Désactiver SSLv2 et SSLv3 et appliquer exclusivement TLS 1.2+ avec suites de chiffrement sécurisées.
- Sécuriser le service VNC avec un mot de passe fort conforme aux bonnes pratiques.
- Vérifier si la machine a déjà été compromise et réinstaller si nécessaire.

En complément, corriger les vulnérabilités de sévérité élevée et moyenne pour réduire la surface d'attaque.

4. Plan d'action

1. **Validation technique :** Vérifier l'applicabilité des correctifs.
2. **Priorisation :** Appliquer immédiatement les correctifs critiques et élevés.
3. **Réévaluation :** Réaliser un nouveau scan après remédiation.
4. **Renforcement :** Mettre en place une stratégie de gestion des correctifs et durcissement.

5. Contexte et méthodologie

L'évaluation a été conduite à l'aide de :

- **Nmap** : cartographie des ports et services exposés, détection de l'OS et des services.
- **Nessus** : analyse des vulnérabilités et génération des scores de sévérité.

La portée est volontairement limitée à l'analyse technique. Aucun test d'exploitation active ni évaluation organisationnelle n'a été effectué.

6. Analyse de risque globale

Les vulnérabilités identifiées exposent la machine à des risques majeurs :

- obtention d'accès non autorisé à des données sensibles,
- perturbation ou interruption des services critiques,
- modification ou destruction d'informations,
- déplacement latéral pour élargir la compromission.

Conclusion : l'état actuel de la machine présente un risque élevé pouvant mener à une compromission complète du système.

7. Annexe technique

Le tableau ci-après présente :

- les ports vulnérables,
- le score de sévérité (CVSS),

- l’ID CVE associé,
- le service concerné,
- la nature de la vulnérabilité,
- la conséquence,
- la remédiation proposée.

Port	Protocole	vulnérabilité	CVE	Risque	CVSS v2.0 Base Score	Service/Produit concerné	Nature de la vulnérabilité	Conséquence principale	recommandations
22, 543 2	tcp	vulnérabilité dans le générateur de nombres aléatoires du package OpenSSH/OpenSSL sur Debian	CVE-2008-0166	Critique	10	OpenSSH/OpenSSL	Faiblesse du générateur de nombres aléatoires dans OpenSSH/OpenSSL sous Debian	écupération de la clé privée de l'hôte et compromission de la confidentialité des sessions SSH	re-générer toutes les clés SSH, SSL et OpenVPN sur le système affecté
23	tcp	Détection de l'utilisation des protocoles SSL versions 2.0 et 3.0	N/A	Critique	10	SSL 2.0 / SSL 3.0	faiblesses cryptographiques connues (padding CBC, renégociation, POODLE).	attaque de type Man-in-the-Middle ou déchiffrement des communications.	Désactiver SSL 2.0/3.0 et forcer l'usage de TLS 1.2+ avec suites robustes
24	tcp	Canonical Ubuntu Linux SEoL (8.04.x)	N/A	Critique	10	canonical Ubuntu 8.04.x	version utilisée arrivée en fin de vie (EoL)	la version utilisé ne reçoit plus de correctifs de sécurité et peut donc contenir des vulnérabilités non corrigées.	Mettre à niveau le système vers une version Ubuntu supportée par l'éditeur (LTS)
25	tcp	Détection de porte dérobée de type Bind Shell	N/A	Critique	10	Port TCP ouvert avec shell non authentifié	shell actif sur un port distant sans authentification	Accès direct et exécution de commandes à distance compromettant le système	Vérifier l'intégrité du système distant. Si compromis, réinstaller le système et sécuriser l'accès aux shells.
5900	tcp	Mot de passe faible pour le serveur VNC	N/A	Critique	10	VNC Server (Virtual Network Computing)	Mot de passe faible / Authentification insuffisante	connection et contrôle total du système	Changer le mot de passe par un mot de passe fort et complexe Activer le chiffrement VNC si disponible Limiter l'accès au serveur via firewall

									ou VPN
8009	tcp	Injection de requête via le connecteur AJP d'Apache Tomcat (Ghostcat), Apache Tomcat SEoL ($\leq 5.5.x$)	CVE-2020-1745, CVE-2020-1938	Critique	10	Apache Tomcat AJP Connector	Lecture de fichiers / Inclusion de fichiers / Possibilité d'exécution de code à distance (RCE)	Accès à des fichiers sensibles et prise de contrôle complète du serveur	Mettre à jour Apache Tomcat vers 7.0.100, 8.5.51, 9.0.31 ou plus récent. Configurer le connecteur AJP pour exiger une authentification. Restreindre l'accès au connecteur AJP aux IP de confiance uniquement. Désactiver AJP si le service n'est pas utilisé.
25, 5432	tcp	Support de suites de chiffrement SSL/TLS de force moyen (Triple DES - vulnérabilité SWEET32)	CVE-2016-2183	Élevée	6.8	SSL/TLS (serveur web)	Support de suites de chiffrement 3DES / Triple DES (ciphers de force moyen, vulnérables à SWEET32)	exploitation de longues sessions pour la récupération des données sensibles en clair	Désactiver les suites de chiffrement 3DES/Triple DES sur le serveur. Utiliser des suites de chiffrement modernes et robustes (AES, ChaCha20). Vérifier la configuration SSL/TLS avec un outil comme SSL Labs.
53	udp	Baisse de performance du service ISC BIND / Déni de service	CVE-2020-8616	Élevée	6.4	ISC BIND (serveur DNS)	Mauvaise limitation du nombre de requêtes (fetches) lors du traitement de réponses DNS	Dégradation du service du serveur DNS (ralentissement ou indisponibilité) et utilisation du serveur comme réflecteur dans une attaque par déni de service	Mettre à jour ISC BIND vers une version corrigée. Limiter l'exposition publique du service.

		réfléchi (Reflected DoS)							DNS récursif Mettre en place un filtrage réseau pour bloquer les requêtes abusives
445	tcp	Vulnérabilité Samba Badlock	CVE- 2016 - 2118	Élevée	6.4	Samba (serveur CIFS/SMB sur Linux/Unix)	Faiblesse dans les protocoles SAM/LSAD due à une mauvaise négociation du niveau d'authentification via RPC	Rétrogradation d'authentification permettant l'exécution d'appels Samba arbitraires et compromission de données ou services	Mettre à jour Samba vers une version corrigée Activer des canaux RPC sécurisés et authentifiés Limiter l'exposition réseau du service SMB/CIFS aux IP de confiance Surveiller et auditer les connexions SMB
2049	tcp	Partage NFS sans restriction d'accès en lecture	N/A	Élevée	6.4	NFS (Network File System) serveur	Partage de répertoires exportés sans restrictions d'accès	Accès non autorisé aux fichiers : lecture, modification ou suppression des données sensibles par un attaquant distant	Restreindre l'accès aux exports NFS par adresse IP/plage IP autorisée appliquer des permissions strictes (lecture/écriture) désactiver les exports inutiles et limiter NFS aux réseaux internes de confiance
22	tcp	Prise en charge de chiffrements faibles par le protocole SSH	N/A	moyen	6.4	Serveur SSH (Secure Shell)	Utilisation de l'algorithme de chiffrement faible Arcfour (RC4) ou absence de chiffrement	interception ou décryptage des communications SSH (perte de confidentialité et intégrité)	Désactiver Arcfour et tout chiffrement non sécurisé dans la configuration SSH (sshd_config) Utiliser uniquement des suites de chiffrement fortes

									(AES, ChaCha20) Mettre à jour le serveur SSH vers une version récente
25	tcp	Expiration du certificat SSL	N/A	moyen	6.1	Services SSL/TLS (HTTPS, FTPS, IMAPS, etc.)	Certificat SSL/TLS arrivé à expiration (ou proche de l'expiration)	Perte de confiance des utilisateurs, erreurs de connexion, interruption potentielle du service sécurisé	Renouveler et remplacer les certificats SSL/TLS avant leur date d'expiration Mettre en place un suivi/alerte automatique sur l'expiration des certificats
25	tcp	Suites de chiffrement SSL faibles prises en charge	N/A	moyen	6.1	chiffrement SSL/TLS (Service SMTP)	Utilisation de suites de chiffrement faibles pour sécuriser les communications	interception et déchiffrement des e-mails (perte de confidentialité et possible manipulation des messages)	Reconfigurer le serveur SMTP pour désactiver les suites de chiffrement faibles n'autoriser que des algorithmes robustes (AES-GCM, CHACHA20, etc.) Mettre à jour la configuration TLS et forcer les versions récentes (TLS 1.2 ou TLS 1.3)
25	tcp	Suites de chiffrement SSL anonymes prises en charge	CVE-2007-1858	moyen	5	SSL/TLS (Service SMTP)	Utilisation de suites de chiffrement anonymes (pas de certificat)	attaque MITM / usurpation de serveur / compromission de la confidentialité et de l'intégrité des e-mails attaques MITM / avertissements de sécurité pour les utilisateurs / perte de confiance dans le service de messagerie.	Reconfigurer le serveur SMTP pour désactiver les suites de chiffrement anonymes Forcer l'utilisation de certificats SSL/TLS valides (issus d'une AC de confiance)

25	tcp	Certificat SSL avec nom d'hôte incorrect	N/A	moyen	5	STARTTLS/SSL (SMTP)	Le certificat SSL/TLS présenté par le serveur possède un CommonName (CN) ou SAN qui ne correspond pas au nom de domaine du service	attaques MITM / avertissements de sécurité pour les utilisateurs / perte de confiance dans le service de messagerie.	Générer ou acheter un certificat SSL/TLS valide dont le CN/SAN correspond exactement au nom du serveur (ex. mail.domaine.com) Déployer ce certificat sur le service SMTP
25	tcp	Certificat SSL non fiable	N/A	moyen	5	STARTTLS/SSL (SMTP)	Le certificat SSL/TLS présenté par le serveur n'est pas fiable : chaîne de confiance rompue, certificat auto-signé, intermédiaire manquant ou signature invalide.	Incapacité du client à vérifier l'identité du serveur, ce qui expose le service à des attaques de type Man-in-the-Middle (MITM) et réduit la confiance des utilisateurs	Obtenir et installer un certificat SSL/TLS valide émis par une autorité de certification reconnue S'assurer que la chaîne complète de certificats (intermédiaires et racine) est correctement configurée et que la signature est valide
25	tcp	Injection de commandes en clair via STARTTLS sur le service SMTP	CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011	moyen	5	STARTTLS/SSL (SMTP)	Faibles dans l'implémentation de STARTTLS permettant l'injection de commandes pendant la phase plaintext qui seront exécutées dans la phase chiffrée.	Vol possible d'e-mails et des identifiants SASL / compromission de la confidentialité et intégrité des communications	Mettre à jour le serveur SMTP avec la dernière version corrigée Appliquer les correctifs pour toutes les CVE listées Vérifier et sécuriser la configuration STARTTLS et SASL. Surveiller les logs pour détecter toute

			- 1432 CVE- 2011 - 1506 CVE- 2011 - 2165						tentative d'exploitation
25	tcp	Certificat SSL auto-signé	N/A	moyen	5	STARTT LS/SSL (SMTP)	La chaîne de certificats X.509 n'est pas signée par une autorité de certification reconnue	Attaque Man-in-the-Middle (MITM) / perte de confiance et interception/modification possible des e-mails.	Acheter ou générer un certificat SSL/TLS valide, émis par une autorité de Certification reconnue, Installer correctement la chaîne complète (certificat serveur + intermédiaires)
25	tcp	Utilisation de chiffrements SSL RC4 vulnérables	CVE- 2013 - 2566 , CVE- 2015 - 280 8	moyen	5	STARTT LS/SSL (SMTP)	Le serveur supporte le chiffre RC4, dont le flux pseudo-aléatoire est biaisé et vulnérable	déduction des informations en clair après l'observation de nombreuses connexions chiffrées, compromettant la confidentialité des e-mails.	Reconfigurer le serveur SMTP pour désactiver RC4 Utiliser des suites de chiffrement robustes (AES- GCM, CHACHA20, etc.) Mettre à jour le serveur pour appliquer les configurations TLS sécurisées.
25	tcp	Suites de chiffrement SSL/TLS EXPORT_RSA ≤ 512 bits prises en	CVE- 2015 - 020 4	moyen	5	chiffrem ent SSL/TLS (Service SMTP)	Support des suites de chiffrement faibles EXPORT_RSA ≤ 512 bits (attaque FREAK)	Forçage d'une connexion avec une clé faible, cassage du chiffrement et lecture ou modification des emails (MITM)	Désactiver le support des suites EXPORT_RSA Autoriser que des chiffrements modernes et

		charge (FREAK)							robustes (ex. AES avec clés ≥ 128 bits)
25	tcp	Vulnérabilité SSL DROWN (Déchiffrement RSA avec un chiffrement obsolète et affaibli)	CVE-2016-0800	moyen	5	chiffrement SSL/TLS (Service SMTP)	Support de SSLv2, exposant le service à l'attaque DROWN	Déchiffrement du trafic TLS impliquant l'interception, lecture ou modification des emails (MITM)	Désactiver complètement SSLv2 et SSLv3 Autoriser que des protocoles sécurisés (TLS 1.2 ou TLS 1.3) Générer un nouveau certificat avec une clé privée non réutilisée si nécessaire
25	tcp	Prise en charge de TLS 1.0 (obsolète et vulnérable)	N/A	moyen	5	chiffrement SSL/TLS (Service SMTP)	Support de TLS 1.0 (protocole obsolète et vulnérable)	perte de confidentialité des communications et non-conformité PCI DSS	Désactiver TLS 1.0 et TLS 1.1 Autoriser uniquement TLS 1.2 et TLS 1.3 Vérifier la compatibilité des clients avant migration
53	tcp	Divulgation d'informations par transferts de zone du serveur DNS (AXFR)	CVE-1999-0532	moyen	5	serveur DNS	Autorisation de DNS Zone Transfer (AXFR) à des hôtes non autorisés	Divulgation d'informations sensibles sur la structure réseau (cartographie interne/externe), aide à la préparation d'attaques ciblées	Restreindre les transferts de zone uniquement aux serveurs DNS secondaires légitimes configurer le serveur DNS pour refuser les requêtes AXFR depuis des hôtes non autorisés
53	udp	Déni de service (DoS) dans ISC BIND	CVE-2020-8617	moyen	5	ISC BIND (serveur DNS)	Vulnérabilité de type Denial of Service (DoS) dans les versions 9.11.18 et antérieures	Indisponibilité du service et interruption de la résolution DNS, Déni de service	Mettre à jour ISC BIND vers une version corrigée ($\geq 9.11.19$, $\geq 9.16.3$, ou version stable la

									plus récente) surveiller les journaux pour détecter d'éventuelles tentatives d'exploitation
53	udp	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	CVE- 202 0- 862 2	moyen	5	ISC BIND (serveur DNS)	échec d'assertion lors de la vérification d'une réponse tronquée à une requête TSIG	Indisponibilité du service et interruption de la résolution DNS par un attaquant distant authentifié, Dénis de service	Mettre à jour ISC BIND vers ≥ 9.11.22, ≥ 9.16.6 ou ≥ 9.17.4 limiter l'utilisation de TSIG uniquement aux hôtes/partenaires de confiance surveiller les logs DNS
80	tcp	Méthodes HTTP TRACE / TRACK Autorisées	CVE- 200 3- 1567 , CVE- 2010 - 038 6, CVE- 200 4- 2320	moyen	5	Serveur Web (HTTP)	Activation des méthodes HTTP TRACE/TRACK	Attaque XST (Cross-Site Tracing) permettant à un attaquant de récupérer des informations sensibles (cookies, entêtes d'authentification)	Désactiver les méthodes TRACE et TRACK dans la configuration du serveur web (Apache, Nginx, IIS, etc.) Appliquer les bonnes pratiques de sécurisation HTTP
445	tcp	Signature SMB non requis	N/A	moyen	4.3	SMB	La signature SMB n'est pas requis	Réalisation d'une attaque Man-in-the- Middle, vol ou modification des données sur le serveur	Activer la signature SMB obligatoire sur le serveur (via la politique de sécurité locale ou les paramètres du serveur) Appliquer les mises à jour de sécurité

									SMB
543 2	tcp	Expiration du certificat SSL	N/A	moyen	4.3	Postgre SQL	Certificat SSL/TLS expiré	Incapacité à vérifier l'identité du serveur, entraînant un risque d'attaque Man-in-the-Middle ou l'interruption des connexions sécurisées	Renouveler ou générer un nouveau certificat SSL/TLS valide pour le serveur PostgreSQL vérifier sa configuration SSL
543 2	tcp	Certificat SSL avec nom d'hôte incorrect	N/A	moyen	4.3	Postgre SQL	Attribut commonName (CN) du certificat SSL ne correspond pas au nom du serveur	Incapacité à vérifier l'identité du serveur, entraînant un risque d'attaque MITM ou interruption des connexions sécurisées	Générer ou acheter un certificat SSL/TLS dont le CN correspond exactement au nom du serveur mettre à jour la configuration PostgreSQL
543 2	tcp	Certificat SSL non fiable	N/A	moyen	4.3	Postgre SQL	Certificat X.509 non fiable	Incapacité à vérifier l'identité du serveur, entraînant un risque d'attaque MITM et perte de confiance dans les connexions sécurisées	Acheter ou générer un certificat SSL/TLS valide provenant d'une CA reconnue Installer la chaîne complète (serveur + intermédiaires) Vérifier les signatures et dates de validité
543 2	tcp	Certificat SSL auto-signé	N/A	moyen	4.3	Postgre SQL	Certificat X.509 auto-signé, non reconnu par une CA	Perte de confiance dans SSL/TLS, entraînant un risque de MITM et interception des communications	Acheter ou générer un certificat SSL/TLS valide auprès d'une CA reconnue installer la chaîne complète (serveur + intermédiaires)

5432	tcp	Support de suites de chiffrement SSL RC4 (Bar Mitzvah)	CVE-2013-2566, CVE-2015-2808	moyen	4.3	PostgreSQL	Support de suites de chiffrement SSL/TLS RC4 faibles	récupération du texte en clair à partir de données chiffrées répétées, entraînant la compromission des communications sécurisées	Désactiver les suites RC4 sur le serveur PostgreSQL Utiliser des suites modernes sécurisées (AES, ChaCha20)
5432	tcp	Détection du protocole TLS version 1.0	N/A	moyen	4	PostgreSQL	Acceptation de connexions avec TLS 1.0, protocole ancien et vulnérable	Communications chiffrées moins sécurisées et risque de non compatibilité avec clients modernes	Désactiver TLS 1.0 sur le serveur Utiliser TLS 1.2 ou TLS 1.3 uniquement
8180	tcp	Fichiers par défaut Apache Tomcat	N/A	moyen	4	Apache Tomcat	Présence de pages d'erreur, index, JSP et servlets par défaut	Fourniture des informations sur le serveur, facilitant la préparation d'attaques ciblées	Supprimer la page d'index par défaut, retirer les JSP et servlets d'exemple remplacer ou modifier les pages d'erreur selon les instructions Tomcat ou OWASP
N/A	icmp	Divulgence de la date distante via requête ICMP Timestamp	CVE-1999-0524	Faible	2.6	Protocole ICMP	Réponse aux requêtes ICMP Timestamp permettant de connaître l'heure système	Divulgence de la date et heure du serveur, entraînant l'aide à contourner les authentifications basées sur le temps	Désactiver les réponses aux requêtes ICMP Timestamp sur le serveur ou filtrer via firewall
22	tcp	Chiffrement en mode CBC activé sur le serveur SSH	CVE-2008-5161	Faible	2.6	SSH	Support de chiffrement CBC, vulnérable à certaines attaques sur le flux chiffré	Récupération du texte en clair, entraînant compromission des données transmises	Désactiver les suites CBC sur le serveur SSH Utiliser des suites plus sécurisées comme AES-GCM ou ChaCha20
22	tcp	Des algorithmes de code d'authentification de	N/A	Faible	2.6	SSH	Support d'algorithmes MAC faibles (MD5 ou 96 bits)	Possibilité de falsification ou modification des données, entraînant la compromission de l'intégrité des communications	Désactiver les MAC faibles Utiliser des MAC plus sécurisés comme SHA-2 ou

		message (MAC) faibles sont activés sur le serveur SSH							SHA-256
22	tcp	Algorithmes d'échange de clés faibles activés sur le serveur SSH	N/A	Faible	2.6	SSH	Support d'algorithmes d'échange de clés faibles (ex. SHA-1, RSA 1024 bits, Diffie-Hellman faible)	Compromission possible des clés et interception des communications, entraînant une perte de confidentialité et d'intégrité	Désactiver les algorithmes faibles Utiliser des algorithmes modernes sécurisés (ex. diffie-hellman-group14-sha256, ecdh-sha2-nistp256)
25, 543 2	tcp	Vulnérabilité POODLE (Padding Oracle On Downgraded Legacy Encryption) dans SSLv3	CVE-2014 - 3566	Faible	2.6	PostgreSQL, SMTP	Le protocole SSLv3 souffre d'une faiblesse dans la gestion du padding CBC	Fuite d'informations sensibles via attaque Man-in-the-Middle ; compromission de sessions chiffrées.	Désactiver totalement le support de SSLv3 sur le serveur (PostgreSQL, SMTP). Activer uniquement TLS 1.2 ou TLS 1.3. Vérifier la compatibilité des clients et mettre à jour ceux qui n'utilisent pas TLS. (Mitigation temporaire) Activer le mécanisme TLS_FALLBACK_SV si disponible.
25	tcp	Suites de chiffrement exportables SSL/TLS EXPORT_DHE ≤ 512 bits prises en charge	CVE-2015 - 4000	Faible	2.1	SMTP	Le service distant accepte des suites de chiffrement EXPORT_DHE avec des clés ≤ 512 bits, vulnérables à la cryptanalyse	Perte de confidentialité et d'intégrité des communications SMTP / Possibilité de déchiffrement des sessions et d'usurpation de messages.	Désactiver la prise en charge des suites de chiffrement EXPORT_DHE et toutes les clés ≤ 1024 bits Configurer

		(Logjam)							uniquement des suites modernes (par ex. TLS_ECDHE avec AES-GCM) et forcer TLS ≥ 1.2
--	--	----------	--	--	--	--	--	--	--

8. Conclusion

Cet assessment a confirmé la présence de vulnérabilités critiques, dont plusieurs alignées avec l'OWASP Top 10. La combinaison de services obsolètes, de faiblesses cryptographiques et de mécanismes d'authentification insuffisants place la machine dans une situation de haut risque.

La mise en œuvre rapide des correctifs recommandés est indispensable pour réduire la surface d'attaque et restaurer un niveau de sécurité acceptable.