

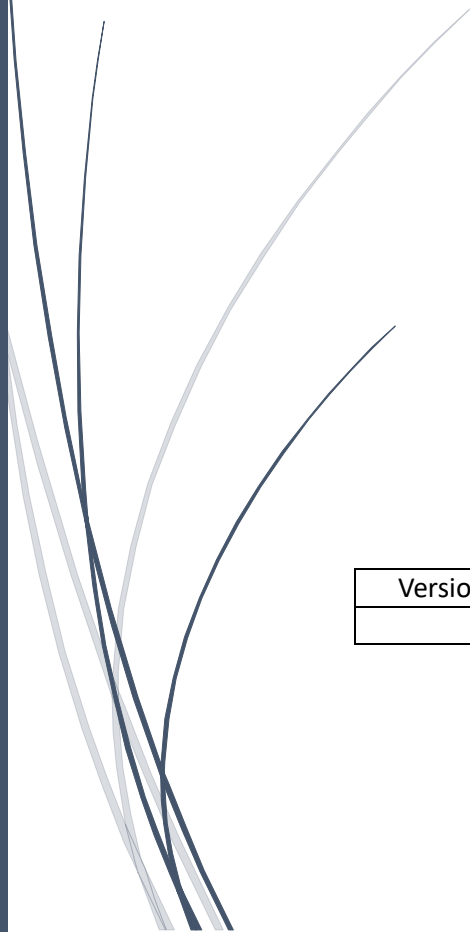
A dark blue vertical bar runs along the left edge of the page. A blue arrow points to the right, overlapping the vertical bar and the title.

Rapport d'Audit de la Sécurité du Système d'Information

De « L'entreprise »

Auditeur chargé de la mission : Benjamin, Tony

Signature :

A stylized, handwritten signature in dark blue ink, consisting of several sweeping, overlapping loops, is positioned below the 'Signature :' label.

Version du document	Date	Diffusion
1.0	05/12/2023	Document Confidentiel

Table des matières

1. Cadre de la mission	2
2.Synthèse Managériale.....	3
3.Références	4
4.Champ d’audit	4
4.1. Liste des Structures à Auditer.....	4
4.2. Description des Systèmes d'Informations.....	4
5.Méthodologie.....	5
6.Présentation des Vulnérabilités.....	6
7.Description et recommandation.....	8
7.1 Pas de Mot de passe Grub	8
7.2 Absence de Configuration de mot de passe	9
7.3 Permission de dossier et fichier	10
7.4 Isolement des partitions.....	11
7.5 Pare-feu non configuré	12
7.6 Configuration SSH manquante.....	13
7.7 Serveur telnet actif.....	15
7.8 Port par default	16
7.9 Pas d’antivirus	17

1. Cadre de la mission

Dans le cadre de la loi n°5 de 2004 et du décret 2004-1250 régissant les normes de sécurité informatique, la présente mission d'audit a été initiée pour évaluer la sécurité de l'infrastructure informatique de [L'entreprise](#). Cette mission d'audit s'inscrit dans le cadre d'un examen exhaustif visant à évaluer la conformité des serveurs Linux par rapport aux standards de sécurité établis.

L'objectif principal de cette mission est de dresser un état de conformité par rapport aux normes établies, d'identifier les vulnérabilités potentielles et les risques de sécurité encourus par l'entreprise. Nous visons également à formuler des recommandations spécifiques et un plan d'action pour renforcer la sécurité de l'infrastructure et des applications concernées.

Notre mission d'audit se concentrera spécifiquement sur l'analyse approfondie des serveurs Linux en recherchant activement les failles potentielles, les lacunes de sécurité et les risques identifiés. Cette évaluation sera réalisée par rapport aux standards métier de référence afin de garantir la robustesse et la fiabilité de l'environnement informatique de [l'entreprise](#).

2.Synthèse Managériale

Audit objectives

The main objective of the audit was to assess the security of the Linux server infrastructure. The audit aimed to identify vulnerabilities, assess compliance with security standards, and make recommendations to reinforce the overall security posture.

Vulnerabilities identified.

During the audit, several vulnerabilities were highlighted, including problems with folder and file permissions, a lack of password and server access security, a failure to isolate partitions, misconfigured potentially dangerous services, and use default ports.

Recommendations

Specific recommendations have been formulated to remedy the identified vulnerabilities. These include configuration adjustments for services, security patches for remote server access, and recommendations for improving password security. Implementing these recommendations will enhance the security of the Linux infrastructure and reduce risks.

3. Références

Les documents et référentiels suivants ont été utilisés comme base pour la réalisation de l'audit :

Guide ANSSI GNU/Linux

Normes et Guides de l'ANSI pour l'Audit de la Sécurité des Systèmes d'Informations

Rapports de Configuration et Bonnes Pratiques du Fabricant Linux

4. Champ d'audit

4.1. Liste des Structures à Auditer

Structure
Serveur Linux

Le périmètre géographique de cette mission d'audit concerne les différentes composantes de l'infrastructure informatique centrale de **l'entreprise**, à savoir le serveurs Linux

Les critères d'échantillonnage ont été définis en prenant en considération l'importance stratégique de chaque composant pour l'activité opérationnelle de l'entreprise, leur interdépendance et leur impact sur la sécurité globale du système d'information.

4.2. Description des Systèmes d'Informations

Serveur Linux

Système d'exploitation Debian 12 avec ses services et rôles spécifiques.

Service SSH

Service Web disponible sur la boucle locale

5.Méthodologie

L'audit sera réalisé en conformité avec le référentiel PASSI (Prestations d'Audit de la Sécurité des Systèmes d'Information) et en se basant sur les guides de sécurité de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ainsi que les standards CIS (Center for Internet Security).

Les outils sélectionnés pour l'audit incluront LinPeas , Nuclei , Lynis et des scripts personnalisés pour évaluer la sécurité du serveur Linux

L'analyse sera réalisée en utilisant des méthodes manuelles et automatisées. Cela comprendra l'examen des configurations, l'analyse des journaux, et l'utilisation d'outils d'évaluation automatisés.

Phase 1 : Collectes d'Informations

Objectifs de la phase : Collecter des informations sur l'infrastructure, y compris la topologie réseau, les services exposés.

Méthodes de collecte d'informations : Scans réseau, analyse des configurations.

Outils utilisés : LinPeas , Nuclei , Lynis, scripts personnalisés.

Livrables attendus : Rapport de collecte d'informations.

Phase 2 : Analyses des Vulnérabilités

Objectifs de la phase : Identifier les vulnérabilités potentielles dans l'infrastructure Linux

Méthodes d'analyse des vulnérabilités : Scans de vulnérabilités, évaluation des configurations.

Outils utilisés : LinPeas , Nuclei , Lynis, scripts personnalisés, ANSSI, PASSI.

Livrables attendus : Rapport d'analyse des vulnérabilités.

Phase 3 : Évaluations des Configurations

Objectifs de la phase : Évaluer les configurations du serveur Linux par rapport aux bonnes pratiques de sécurité.

Méthodes d'évaluation des configurations : Examen manuel des paramètres de sécurité, utilisation de guides de référence.

Outils utilisés : LinPeas , Nuclei , Lynis, scripts personnalisés, ANSSI, PASSI.

Livrables attendus : Rapport d'évaluation des configurations.

6.Présentation des Vulnérabilités

Facilité d'exploitation / Impact	Difficile	Elevée	Modérée	Facile
Mineur	Mineur	Mineur	Important	Majeur
Important	Mineur/Important	Important	Important	Majeur
Majeur	Important	Majeur	Majeur	Critique
Critique	Important	Majeur	Critique	Critique

Serveur Linux

Titre	Description	Preuve	Niveau de risque
Mot de passe GRUB	Pas de mot de passe sur le GRUB	7.1	Important
Absence de configuration de mot de passe	Pas de configuration / module pour durcir les mots de passes	7.2	Important
Isolement des partitions	Certaines partitions peuvent être facilement remplies par les utilisateurs	7.4	Important
Port par défaut	Les ports SSH et Telnet sont par défaut	7.8	Important
Pare-feu	Pare-feu activé mais aucune règle configurée	7.5	Majeur

Titre	Description	Preuve	Niveau de risque
SSH configuration	Manque de configuration SSH	7.6	Majeur
Permission fichier sudoers.d et /home	Fichier sudoers.d et dossier /home accessible par tout le monde	7.3	Majeur
Pas d'antivirus	Pas d'antivirus installer	7.9	Majeur
Telnet server actif	Service Telnet actif	7.7	Critique

7.Description et recommandation

7.1 Pas de Mot de passe Grub

Description

L'absence de mot de passe pour GRUB expose le système à des attaques potentielles au niveau du gestionnaire de démarrage.

Recommandations

Configurer un mot de passe pour GRUB pour renforcer la sécurité du démarrage.

Mettre en œuvre des restrictions d'accès physique au serveur pour prévenir l'accès non autorisé au gestionnaire de démarrage.

Preuve

```
GNU nano 5.4 /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet"
GRUB_CMDLINE_LINUX=""

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command `vbeinfo`
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at grub start
#GRUB_INIT_TUNE="480 440 1"
```

7.2 Absence de Configuration de mot de passe

Description

L'absence de configurations de mot de passe peut entraîner des risques de sécurité majeurs en permettant un accès non autorisé aux comptes utilisateur et aux comptes de services.

Recommandations

Utiliser des Module PAM (Pluggable Authentication Modules) appropriés pour imposer des critères de complexité (longueur, caractères spéciaux, etc.) et Configurer des politiques de mot de passe PAM strictes.

Configurer la durée de validité des mots de passe avec le module pam_unix.

Mettre en place des politiques de verrouillage de compte après un certain nombre de tentatives infructueuses.

Module PAM : Utilisez le module pam_unix.so dans le fichier de configuration /etc/pam.d/common-password pour spécifier les paramètres de mot de passe.

Preuve

```
- Checking user password aging (minimum) [ DÉSACTIVÉ ]
- User password aging (maximum) [ DÉSACTIVÉ ]
- Checking expired passwords [ OK ]
- Checking Linux single user mode authentication [ OK ]
- Determining default umask
  - umask (/etc/profile) [ NON TROUVÉ ]
  - umask (/etc/login.defs) [ SUGGESTION ]
- LDAP authentication support [ NON ACTIVÉ ]
- Logging failed login attempts [ ACTIVÉ ]
```

7.3 Permission de dossier et fichier

Description

Des autorisations inappropriées sur des fichiers et des répertoires, tels que /home et /etc/sudoers.d, peuvent conduire à des fuites d'informations sensibles et à des vulnérabilités d'exécution de code.

Recommandations

Répertoire /home :

Limiter l'accès au répertoire /home aux utilisateurs propriétaires et aux administrateurs système.

S'assurer que les permissions sur les dossiers utilisateur individuels (/home/utilisateur) sont correctement configurées pour éviter tout accès non autorisé.

Fichier /etc/sudoers.d :

Restreindre l'accès en écriture à ce répertoire aux utilisateurs du groupe sudo.

S'assurer que les fichiers dans ce répertoire ont des permissions appropriées, généralement accessibles en lecture uniquement pour les administrateurs.

Preuve

```
tony@SRV-Deb:~$ sudo ls -l /home
[sudo] Mot de passe de tony :
total 8
drwxr-xr-x  2 benjamin benjamin 4096  4 oct.  13:21 benjamin
drwxr-xr-x 19 tony      tony     4096 18 janv. 09:25 tony
tony@SRV-Deb:~$ sudo ls -l /etc/sudoers.d
total 4
-r--r----- 1 root root 958 14 janv.  2023 README
tony@SRV-Deb:~$ sudo ls -l /etc/ | grep sudo
-rw-r--r--  1 root root  3975 14 janv.  2023 sudo.conf
-r--r----- 1 root root   692  4 oct.  11:45 sudoers
drwxr-xr-x  2 root root  4096  4 oct.  11:35 sudoers.d
-rw-r--r--  1 root root  6169 14 janv.  2023 sudo_logsrvd.conf
tony@SRV-Deb:~$
```

7.4 Isolement des partitions

Description

L'isolement insuffisant des partitions, en particulier pour /home, /tmp et /var, peut entraîner une propagation de l'infection en cas de compromission.

Recommandations

Partition /home :

Isoler /home /tmp et /var sur des partitions distinctes.

Appliquer des restrictions d'accès strictes, limitant l'accès aux utilisateurs autorisés.

Utiliser l'option noexec pour empêcher l'exécution de fichiers binaires dans /tmp.

Preuve

```
tony@SRV-Deb:~$ df -h
df: /run/user/1000/doc: Opération non permise
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                944M      0  944M   0% /dev
tmpfs               194M    1,1M  193M   1% /run
/dev/sda1           58G     5,5G   50G  10% /
tmpfs               968M    696K  967M   1% /dev/shm
tmpfs               5,0M     4,0K  5,0M   1% /run/lock
tmpfs               194M    844K  193M   1% /run/user/1000
tony@SRV-Deb:~$ cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point> <type> <options>          <dump> <pass>
# / was on /dev/sda1 during installation
UUID=3b87458d-08c8-4f4d-98cd-0842eaa7ed99 /          ext4      errors=remount-ro 0      1
# swap was on /dev/sda5 during installation
UUID=0c2c8a4c-ea7a-428e-b535-073f9f7425c0 none        swap      sw          0      0
/dev/sr0          /media/cdrom0  udf,iso9660 user,noauto 0        0
```

7.5 Pare-feu non configuré

Description

Un pare-feu non configuré expose le serveur à des attaques réseau non autorisées.

Recommandations

Configurer le pare-feu pour filtrer le trafic réseau entrant et sortant.

Autoriser uniquement les ports nécessaires pour les services essentiels.

Bloquer le trafic non autorisé ou non nécessaire.

Preuve

```
tony@SRV-Deb:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
tony@SRV-Deb:~$
```

7.6 Configuration SSH manquante

Description

La configuration actuelle de SSH comporte des éléments suggérant des améliorations pour renforcer la sécurité du service.

Recommandations

AllowTcpForwarding	Considérez de définir cette option en fonction des besoins spécifiques de votre environnement pour éviter des risques liés à la redirection de port.
ClientAliveCountMax	Définissez un nombre maximal d'essais après lesquels le serveur terminera une session inutilisée pour renforcer la sécurité contre les sessions inactives.
Compression	Désactivez la compression si elle n'est pas nécessaire pour économiser la bande passante.
LogLevel	Définissez un niveau de journalisation approprié pour les besoins de suivi et de débogage.
MaxAuthTries	Limitez le nombre maximal de tentatives d'authentification pour renforcer la résistance aux attaques par force brute.
MaxSession	Limitez le nombre maximal de sessions par connexion
TCPKeepAlive	Activez TCPKeepAlive pour gérer les connexions inactives
Port	Considérez de changer le port SSH par défaut (22) pour minimiser les attaques automatisées.
X11Forwarding	Désactivez si vous n'avez pas besoin de transfert X11
AllowAgentForwarding	Désactivez si vous n'avez pas besoin de transfert d'agent.
AllowUsers	Définissez une liste restreinte d'utilisateurs autorisés à se connecter.
AllowGroups	Définissez une liste restreinte de groupes autorisés à se connecter.

Preuve

```
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem      sftp      /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server
```

7.7 Serveur telnet actif

Description

Telnet transmet les informations, y compris les mots de passe, de manière non cryptée, présentant des risques de sécurité importants.

Recommandations

Désactiver Telnet

Preuve

```
tony@SRV-Deb:~$ nmap 192.168.100.132
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-18 12:43 CET
Nmap scan report for 192.168.100.132
Host is up (0.000091s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
7070/tcp   open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
tony@SRV-Deb:~$ sudo dpkg -l | grep telnet
ii telnet          0.17-42          amd64          basic telnet client
ii telnetd         0.17-42          amd64          basic telnet server
tony@SRV-Deb:~$
```


7.8 Port par default

Description

Utiliser des ports par défaut peut exposer le serveur à des scans automatisés et à des attaques ciblées, ici le port 22 et 23 sont utilisés.

Recommandations

Changer les ports par défaut pour les services afin de compliquer les attaques automatisées.

Utiliser des ports non standards pour les services critiques.

Preuve

```
tony@SRV-Deb:~$ sudo netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
tcp 0 0 127.0.0.1:4000 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:41462 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:3000 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:7070 0.0.0.0:* LISTEN
tcp6 0 0 :::1:4000 :::* LISTEN
tcp6 0 0 :::22 :::* LISTEN
tcp6 0 0 :::1:631 :::* LISTEN
tcp6 0 0 :::1:3000 :::* LISTEN
udp 0 0 0.0.0.0:50001 0.0.0.0:*
udp 0 0 0.0.0.0:68 0.0.0.0:*
udp 0 0 0.0.0.0:49271 0.0.0.0:*
udp 0 0 0.0.0.0:5353 0.0.0.0:*
udp 0 0 0.0.0.0:631 0.0.0.0:*
udp6 0 0 :::60641 :::*
udp6 0 0 :::5353 :::*
```

```
tony@SRV-Deb:~$
```

7.9 Pas d'antivirus

Description

L'absence d'un antivirus expose le serveur à des risques liés aux malwares et aux attaques par logiciels malveillants.

Recommandations

Installer et configurer un logiciel antivirus adapté au système d'exploitation Debian 12.

Effectuer des analyses régulières pour détecter et éliminer les menaces potentielles.

Preuve