

SOMMAIRE



I. Présentation de l'entreprise



II. Projets

- 1) Hackathon
- 2) OVH/Mails
- 3) ISPConfig
- 4) Backup serveur
- 5) Serveur Linux
- 6) Cybersécurité
- 7) Base de données MySQL



III. Conclusion

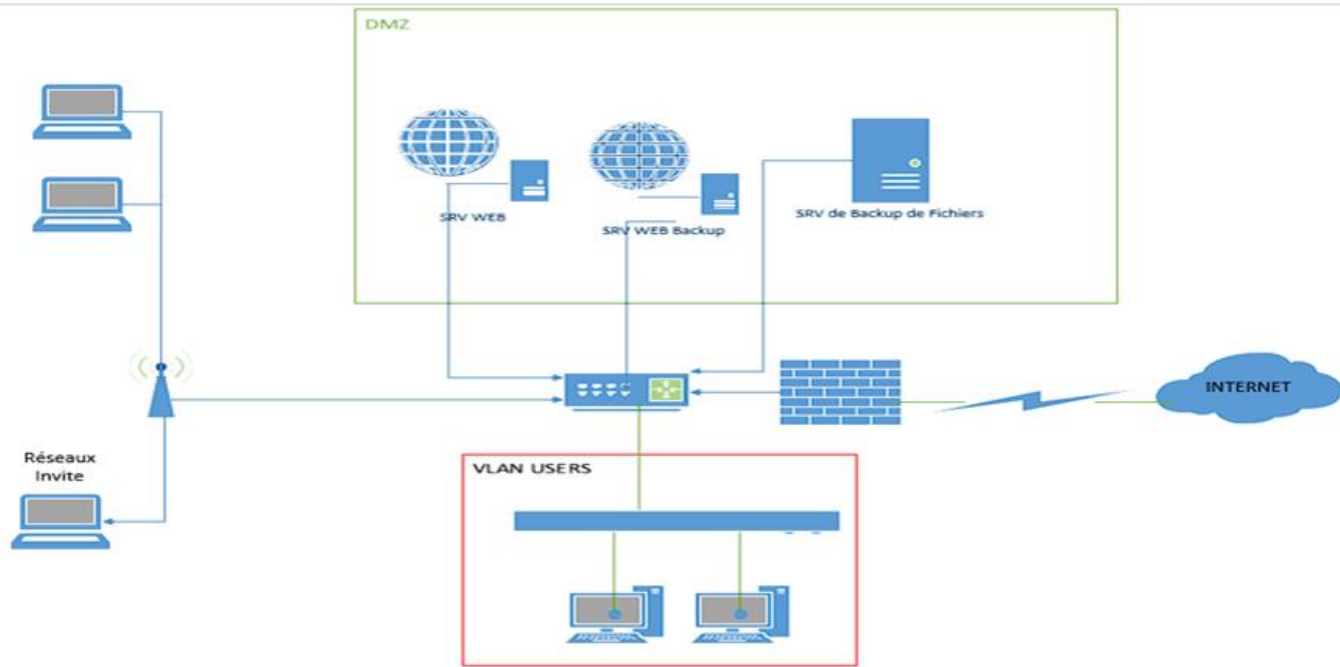
I. PRÉSENTATION DE L'ENTREPRISE



Dénomination sociale : SLD-CSVI

Siège sociale : 8, avenue de la Gare, 95380 Louvres

Objectif : récolter des fonds afin de contribuer au développement d'une plateforme e-santé (carnet de santé virtuel et intelligent) , qui améliorera les conditions de prise en charge des patients auprès des professionnels de santé, et tous objets similaires, connexes ou complémentaires ou susceptibles d'en favoriser la réalisation ou le développement



1) HACKATHON

- Créations des Vlan
- Configuration routeur WI-Fi
- Audit de sécurité
- Attaques

nessus Essentials

Scans Settings

Back to My Scans

Hosts 1 Vulnerabilities 14 Notes 3 VPR Top Threats History 1

Filter Search Vulnerabilities 14 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	5.3	SMB Signing not required	Misc.	1
INFO	—	SMB (Multiple Issues)	Windows	5
INFO	—	Microsoft Windows (Multiple Issues)	Windows	2
INFO	—	DCE Services Enumeration	Windows	9
INFO	—	Common Platform Enumeration (CPE)	General	1
INFO	—	Device Type	General	1
INFO	—	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	—	Nessus Scan Information	Settings	1
INFO	—	OS Identification	General	1
INFO	—	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)	Misc.	1
INFO	—	OS Security Patch Assessment Available	Settings	1
INFO	—	Target Credential Issues by Authentication Protocol - No Issues Found	Settings	1
INFO	—	Target Credential Status by Authentication Protocol - Valid Credentials Provided	Settings	1
INFO	—	VMware ESX/GSX Server detection	Service detection	1

Scan Details

Policy: Advanced Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Tenable News

Cross-site Scripting in webapp.kalza.la and kalza.la... [Read More](#)

58
of 100

+ NEW TEST

MailGenius Score

We've found 7 thing(s) you can do to avoid landing in the spam folder and increase security.

However, there are several other factors that go into deliverability such as domain reputation, list hygiene etc., which play a large role when inboxing. You can be authenticated and follow best practices, but if recipients mark your emails as spam, they'll be classified as spam.

Email from: contact@savelifedata.com 23/05/2022

Subject: test

Don't lose money to the Spam Folder

Set Up A Free Call To Learn More

Work with Email Deliverability Experts to solve your email issues.

7 THINGS TO FIX

EMAIL PREVIEW

SEVERITY	TEST	DESCRIPTION
● Failing -18	Domain Blacklists	Your domain is listed on significant blacklists.
● Failing -8	IP Blacklists	Your Mail Server IP address is listed on significant blacklists.
● Failing -5	DMARC	Your DMARC authentication is not setup using best practices.
● Failing -4	SPF	Your SPF record has errors.
● Failing -4	DKIM	Your DKIM key has errors.

91
of 100

+ NEW TEST

MailGenius Score

We've found 4 thing(s) you can do to avoid landing in the spam folder and increase security.

However, there are several other factors that go into deliverability such as domain reputation, list hygiene etc., which play a large role when inboxing. You can be authenticated and follow best practices, but if recipients mark your emails as spam, they'll be classified as spam.

Email from: contact@savelifedata.com 27/05/2022

Subject: test 27/05/22

Don't lose money to the Spam Folder

Set Up A Free Call To Learn More

Work with Email Deliverability Experts to solve your email issues.

4 THINGS TO FIX

EMAIL PREVIEW

SEVERITY	TEST	DESCRIPTION
● Failing -4	DKIM	Your DKIM key has errors.
● Warning -3	DMARC	Your DMARC authentication is not setup using best practices.
● Warning -1	List-Unsubscribe Header	Your email is missing the List-Unsubscribe header.
● Warning -1	SpamAssassin	Your SpamAssassin score is approaching the spam threshold.
● Passing	SPF	Your SPF record looks great!

2) OVH/MAILS

- Création de scripts en PHP (fonction mail et PHP Mailer)
 - Diagnostic état des mails (Mail Genius)
 - Mise en place des solutions pour solutionner le problème des mails
 - DNS (Enregistrements DKIM, SPF et DMARC)
- Configuration des mails sur ISPConfig
- <https://savelifedata.com/PHPMailer/>

3) ISPCONFIG

ISPConfig est une interface de gestion de serveur pour Linux.

ISPConfig simplifie la gestion des différents services liés à l'hébergement web tel que la configuration DNS, la gestion des noms de domaines, le courrier électronique ou le transfert de fichiers FTP.

- Configuration du DNS (Enregistrements)
- Application d'un certificat SSL (Lests Encrypt)
- Backup sur ISPConfig

The screenshot displays the ISPConfig web interface. At the top, there is a search bar labeled 'Rechercher' and a red button labeled 'SE DÉCONNECTER ADMIN'. Below this is a navigation menu with icons for Accueil, Client, Sites, E-mail, DNS (highlighted in red), Suivi, Aide, Outils, and Système. On the left side, there is a sidebar menu with options: Assistant DNS, Ajout zone DNS, Importer un fichier de Zone, Modèles, DNS (highlighted), Zones, Secondary DNS, and Zones secondaires. The main content area is titled 'Zone DNS' and contains two tabs: 'Enregistrements' (selected) and 'Zone settings'. Under the 'Enregistrements' tab, there is a grid of buttons for various DNS record types: A, AAAA, ALIAS, CAA, CNAME, DNAME, DKIM, DS, DMARC, HINFO, LOC, MX, NAPTR, NS, PTR, RP, SPF, SRV, SSHFP, TLSA, and TXT. Below this grid is a table with columns: Actif, Type, Nom, Données, Priorité, and TTL. The table has a dropdown menu for '1.' in the top right corner. The first row of the table shows a record for 'savelifedata.com' with IP address '54.38.35.112', priority '0', and TTL '3600'. There is a red trash icon at the end of the row.

Actif	Type	Nom	Données	Priorité	TTL
Oui	A	savelifedata.com.	54.38.35.112	0	3600

4) BACKUP SERVEUR



Réalisation d'un backup complet du serveur Linux avec la commande tar



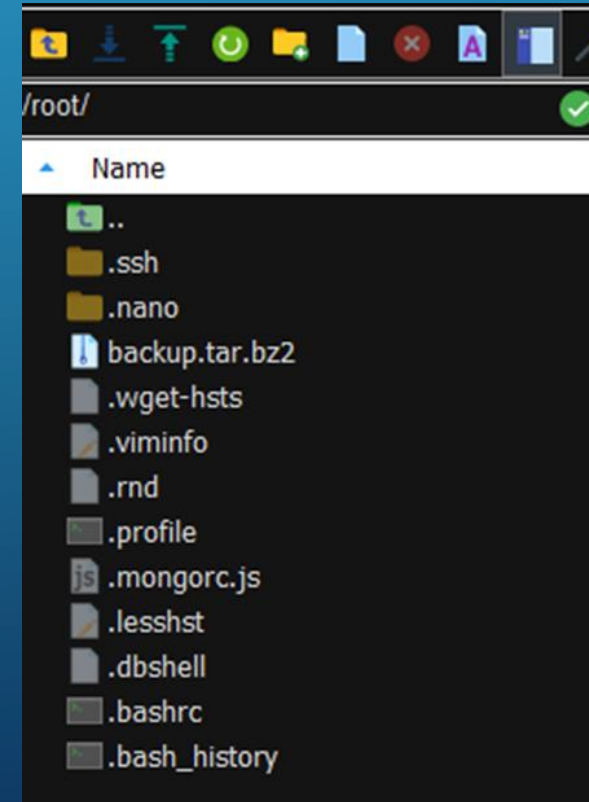
```
tar cvpjf backup.tar.bz2 --  
exclude=/proc --exclude=/lost+found -  
-exclude=backup.tar.bz2 --  
exclude=/mnt --exclude=/sys --  
exclude=/boot /
```



Restauration du backup sur une machine virtuelle



Tutoriel : <https://www.it-connect.fr/linux-sauvegarder-et-restaurer-son-systeme/>

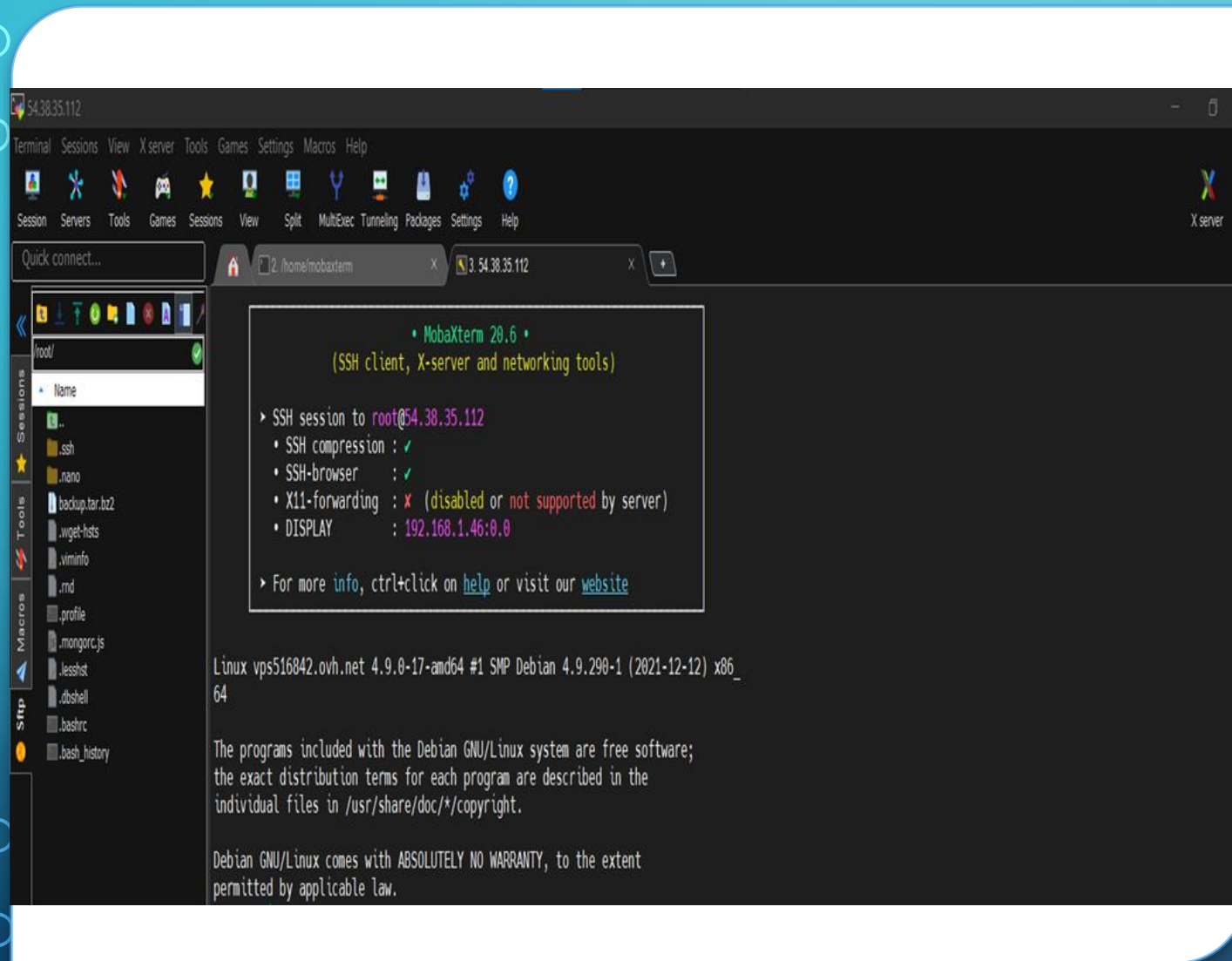


5) SERVEUR LINUX

L'accès au serveur linux se faisait par SSH avec le logiciel MobaXterm.

MobaXterm est un émulateur de terminal Linux qui propose divers outils comme le SSH, FTP...

- Liste qui répertorie l'ensemble des applications installées sur le serveur
 - Check-lists points de sécurité à vérifier sur le serveur





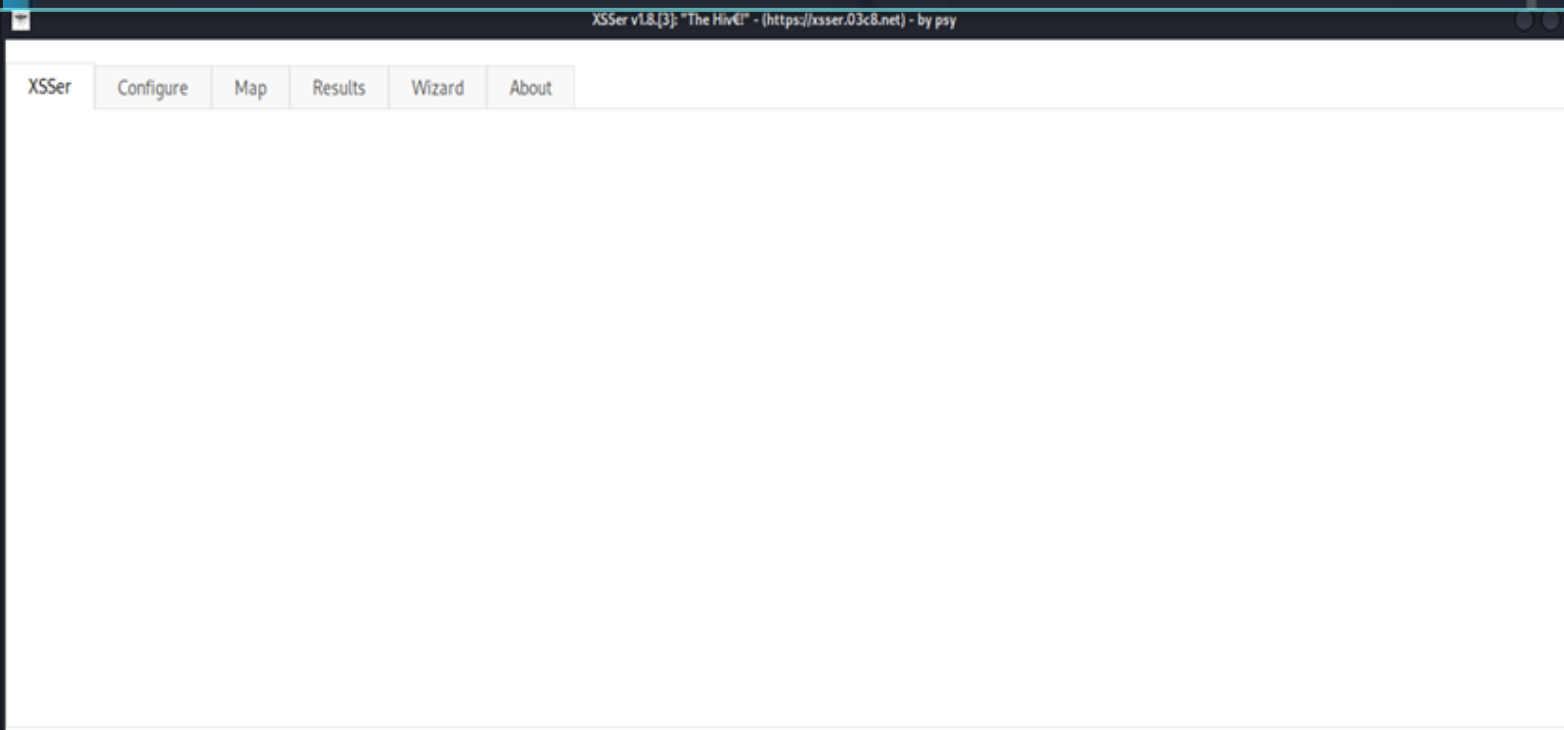
```
root@kali: /home/kali
File Actions Edit View Help

PENTMENU

Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding

1) Recon      3) Extraction  5) Quit
2) DOS        4) View Readme

Pentmenu>
```



6) CYBERSÉCURITÉ

- Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service en le faisant crasher. Pour ce faire, l'attaquant utilise un logiciel qui envoie beaucoup trop de paquets (demande) par seconde au serveur victime.

- Pentmenu

- L'attaque XSS, également appelée cross-site Scripting est une attaque qui consiste en le fait d'exploiter une faille du site afin de pouvoir injecter du code malveillant en HTML ou en JavaScript dans des variables qui sont mal protégées.

- XSSER

https://savelifedata.com/phpmyadmin/server_import.php?db=&token=8eed1b5e99dfaf0aa15a5c4a88b38748

MyAdmin

Préférences

le base de données

onfig

ation_schema

mance_schema

cube

Serveur: localhost:3306

Bases de données SQL État Comptes d'utilisateurs Export

Importation dans le serveur actuel

Fichier à importer :

Le fichier peut être comprimé (gzip, bzip2, zip) ou non.
Le nom du fichier comprimé doit se terminer par **[format].[compression]**. Exemple: **.sql.zip**

☐ Parcourir : Aucun fichier n...été sélectionné (Taille maximum: 10 Mo)
Vous pouvez également faire glisser et déposer un fichier sur n'importe quelle page.

☐ Choisissez depuis le répertoire de téléchargement du serveur web **/etc/phpmyadmin**

Jeu de caractères du fichier :

Importation partielle :

☒ Permettre l'interruption de l'importation si la limite de temps configurée dans PHP est sur le point d'être atteinte (*transactions*.)

Ignorer ce nombre de requêtes (pour SQL), à partir du début :

Autres options :

☒ Activer la vérification des clés étrangères

7) BASE DE DONNÉES MYSQL

- Conception d'un répertoire de téléchargement, plutôt que de passer par l'envoi de fichier traditionnel dans le formulaire d'importation, afin de pouvoir restaurer le dump d'une sauvegarde SQL et de contourner les limites d'envoi et de réception de fichiers
- Configuration du fichier php.ini d'Apache2 pour permettre l'importation de bases de données qui ont une taille importante

- Mes impressions :
 - Découvrir plus en détail le milieu professionnel
 - Développer mes compétences (Gérer le patrimoine informatique, travailler en mode projet...)
 - Préparer au passage des épreuves (E4,E5...)

Avez-vous des questions ?

III. CONCLUSION