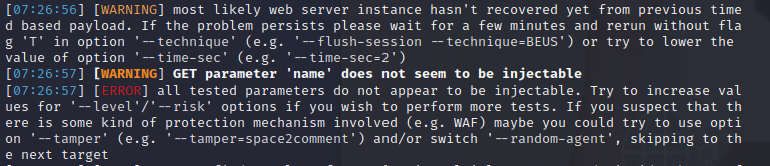
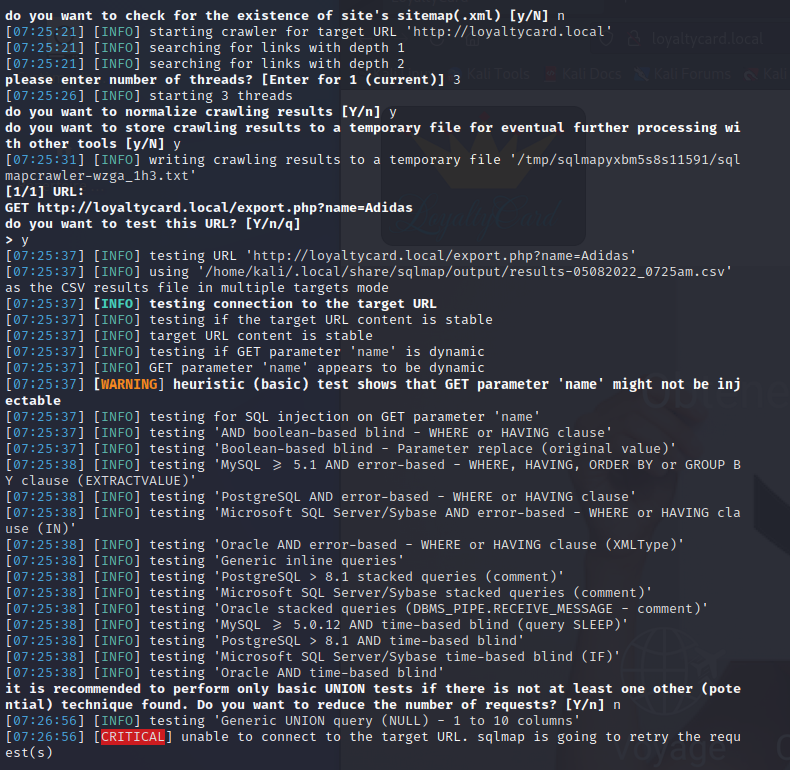
Analyse du serveur Web avec Nikto :Une image contenant texte

Description générée automatiquement

Serveur Web de type Apache, avec la version 2.4.48 sur une machine Debian répondant sur le port 80.

|  |  |
| --- | --- |
| Failles | Risques réels |
| Cookie PHPSESSID créé sans httponly | Accès aux cookies en Javascript |
| Réponse valide méthodes HTTP | Faux positifs |
| OSVDB-3092 | Manuel du serveur web trouvé |
| OSVDB-3268 | Indexation de répertoire trouvé |

Test de pénétration de détection et d’exploitation des failles d’injection SQL avec Sqlmap :



Résultats :

Test sur l’url ‘http://loyaltycard.local/export.php?name=Adidas’

* URL stable
* Paramètre Get ‘name’ est dynamique donc ne peux pas être injectable

Test d’ajout de paramètre après une ligne SQL pour plusieurs BDD :

* Erreur pour toutes les bases de données testées

Résultat final :

« Tous les paramètres testés ne semblent pas injectables »

Vérification des ports ouverts sur les différents réseaux :

Une image contenant texte

Description générée automatiquementNmap du réseau 192.168.10.0/24 (DMZ) :

|  |  |
| --- | --- |
| Machine/IP | Ports ouvert |
| Base de données (192.168.10.2) | * 22 => connexion SSH * 80 => http * 3306 => Mysql |
| Serveur Web (192.168.10.5) | * 22 => connexion SSH * 80 => http * 443 => http ssl |
| Interface Firewall (192.168.10.253) | * 53 => DNS * 80 => http |
| Interface Firewall (192.168.10.254) | * 53 => DNS * 80 => http |
| Interface Firewall VIP (192.168.10.100) | * 53 => DNS * 80 => http |

Nmap du réseau 192.168.20.0/24 (Lan site 1) :

Une image contenant texte

Description générée automatiquement

|  |  |
| --- | --- |
| Machine/IP | Ports ouvert |
| Base de données (192.168.20.50) | * 3306 => Mysql |
| Interface Firewall (192.168.20.253) | * 53 => DNS |
| Interface Firewall (192.168.20.254) | * 53 => DNS |
| Interface Firewall (192.168.20.100) | * 53 => DNS |
| Active Directory et la machine client | * 53 => DNS * 80 => http |

Nmap identique pour les autres réseaux qui sont configurés de la même façon que le Lan site 1.