

# Guide d'Utilisation des Outils d'Audit de Sécurité

## Introduction

Dans le contexte actuel de cybermenaces croissantes, la sécurité informatique est une préoccupation majeure pour toutes les entreprises. Les audits de sécurité réguliers sont essentiels pour identifier et corriger les vulnérabilités avant qu'elles ne soient exploitées par des acteurs malveillants. Ce guide vous présente cinq outils open-source sélectionnés pour leur efficacité et leur polyvalence, vous permettant de fournir des services d'audit de sécurité complets et de qualité à vos clients.

## Choix des outils

La sélection de ces outils a été guidée par plusieurs critères :

- **Efficacité** : Chaque outil a fait ses preuves dans la détection de vulnérabilités spécifiques.
- **Polyvalence** : Ils couvrent un large éventail de domaines de la sécurité informatique.
- **Open-Source** : Leur nature gratuite permet une utilisation flexible et adaptable à différents budgets.
- **Communauté active** : Ils bénéficient pour la plupart d'une communauté d'utilisateurs et de développeurs importante, garantissant un support et des mises à jour régulières.

## Cas d'usage

Chaque outil répond à des besoins spécifiques en matière d'audit de sécurité :

- **OpenVAS** : Idéal pour l'évaluation complète de la sécurité des infrastructures réseau, la détection de vulnérabilités connues sur les serveurs, les applications et les équipements réseau.
- **Zaproxy** : Essentiel pour auditer la sécurité des applications web, en identifiant les failles courantes telles que les injections SQL et les scripts intersites (XSS).
- **Wifite** : Spécialisé dans l'audit des réseaux Wi-Fi, permettant de tester la robustesse des protocoles de sécurité et d'identifier les points d'accès vulnérables.
- **ScubaGear** : Conçu pour analyser la sécurité des environnements Office 365, en vérifiant les configurations, les permissions et les activités suspectes.
- **Domain\_Audit** : Indispensable pour auditer Active Directory, en détectant les mauvaises configurations, les comptes vulnérables et les problèmes de sécurité liés aux privilèges.

## Objectifs de la démarche d'audit

L'utilisation combinée de ces outils vous permet d'atteindre les objectifs suivants :

- **Identifier les vulnérabilités** : Détecter les failles de sécurité, les erreurs de configuration et les mauvaises pratiques qui pourraient être exploitées par des attaquants.
- **Évaluer les risques** : Analyser l'impact potentiel de chaque vulnérabilité sur les activités de l'entreprise et prioriser les actions correctives.
- **Recommander des solutions** : Proposer des mesures concrètes et adaptées pour corriger les vulnérabilités et renforcer la sécurité globale du système d'information.
- **Apporter une valeur ajoutée** : Fournir à vos clients un audit complet et professionnel, démontrant votre expertise en matière de sécurité informatique.

En suivant ce guide, vous serez en mesure d'utiliser ces outils de manière efficace pour fournir des audits de sécurité de qualité à vos clients, contribuant ainsi à protéger leurs actifs numériques et à renforcer leur confiance en vos services.

## TABLE DES MATIÈRES

<b>1. OpenVAS</b>	<b>3</b>
Présentation	3
Cas d'usage d'OpenVAS :	3
OpenVAS : Scans Internes vs. Scans Externes	4
Fonctionnement	4
Guide d'utilisation détaillé	4
1. Lancement de l'interface web :	4
2. Configuration d'un nouveau scan :	5
3. Création d'une tâche (Task) :	6
4. Exécution du scan :	6
5. Analyse des résultats :	6
Explications supplémentaires sur les rapports OpenVAS	7
<b>2. Zaproxy</b>	<b>8</b>
Présentation	8
Cas d'usage de Zaproxy :	8
Zaproxy : Scans Externes pour Applications Web	8
Fonctionnement	9
Guide d'utilisation détaillé	9
1. Lancement de ZAP : Ouvrez ZAP depuis votre menu d'applications ou en ligne de commande.	9
2. Scan :	9

3. Génération de rapports :	10
Explications supplémentaires sur les rapports Zaproxy	11
<b>3. Wifite</b>	<b>12</b>
Présentation	12
Cas d'usage de Wifite :	12
Fonctionnement	12
Guide d'utilisation détaillé	13
1. Lancement de Wifite :	13
2. Sélection des réseaux cibles :	13
3. Lancement des attaques :	13
4. Analyse des résultats :	13
Explications supplémentaires sur les attaques Wifite	13
<b>4. ScubaGear</b>	<b>14</b>
Présentation	14
Cas d'usage de ScubaGear :	14
Guide d'utilisation détaillé	15
1. Connexion à Office365 :	15
2. Analyse des résultats :	15
Explications supplémentaires sur les audits ScubaGear	16
<b>5. Domain_Audit</b>	<b>16</b>
Présentation	16
Cas d'usage de Domain_Audit :	16
Exemples Concrets d'Utilisation :	16
Fonctionnement	17
Guide d'Utilisation Détaillé	17
1. Exécution de l'audit :	17
2. Analyse des résultats :	17
Interprétation des Résultats	19

## 1. OpenVAS

### Présentation

OpenVAS (Open Vulnerability Assessment System) est un outil open-source incontournable pour la gestion des vulnérabilités. Il permet de scanner en profondeur les réseaux, serveurs et applications afin de détecter les failles de sécurité qui pourraient être exploitées par des attaquants. Grâce à sa base de données complète et régulièrement mise à jour, OpenVAS est capable d'identifier un large éventail de vulnérabilités connues, qu'elles soient liées aux logiciels, aux configurations ou aux mauvaises pratiques.

## Cas d'usage d'OpenVAS :

- **Audits de sécurité réguliers** : Pour évaluer en continu la posture de sécurité d'une entreprise et identifier les nouvelles vulnérabilités.
- **Tests d'intrusion** : Pour simuler des attaques et évaluer la capacité du système à résister aux intrusions.
- **Évaluation de la conformité** : Pour vérifier si l'infrastructure respecte les normes de sécurité en vigueur (PCI DSS, ISO 27001, etc.).
- **Analyse de vulnérabilités avant et après l'application de correctifs** : Pour mesurer l'efficacité des mesures de sécurité mises en place.

## OpenVAS : Scans Internes vs. Scans Externes

OpenVAS permet de réaliser deux types de scans complémentaires :

- **Scans internes** : Ciblent les systèmes et les réseaux internes de l'entreprise. Ils permettent d'identifier les vulnérabilités qui pourraient être exploitées par un attaquant ayant déjà accès au réseau interne (par exemple, un employé malveillant ou un logiciel malveillant).
- **Scans externes** : Ciblent les services et les applications exposés sur Internet. Ils permettent d'identifier les vulnérabilités accessibles depuis l'extérieur, qui pourraient être exploitées par des attaquants distants.

En combinant ces deux types de scans, OpenVAS offre une vision complète de la surface d'attaque d'une entreprise, permettant ainsi de mettre en place des mesures de sécurité adaptées pour protéger l'ensemble de l'infrastructure.

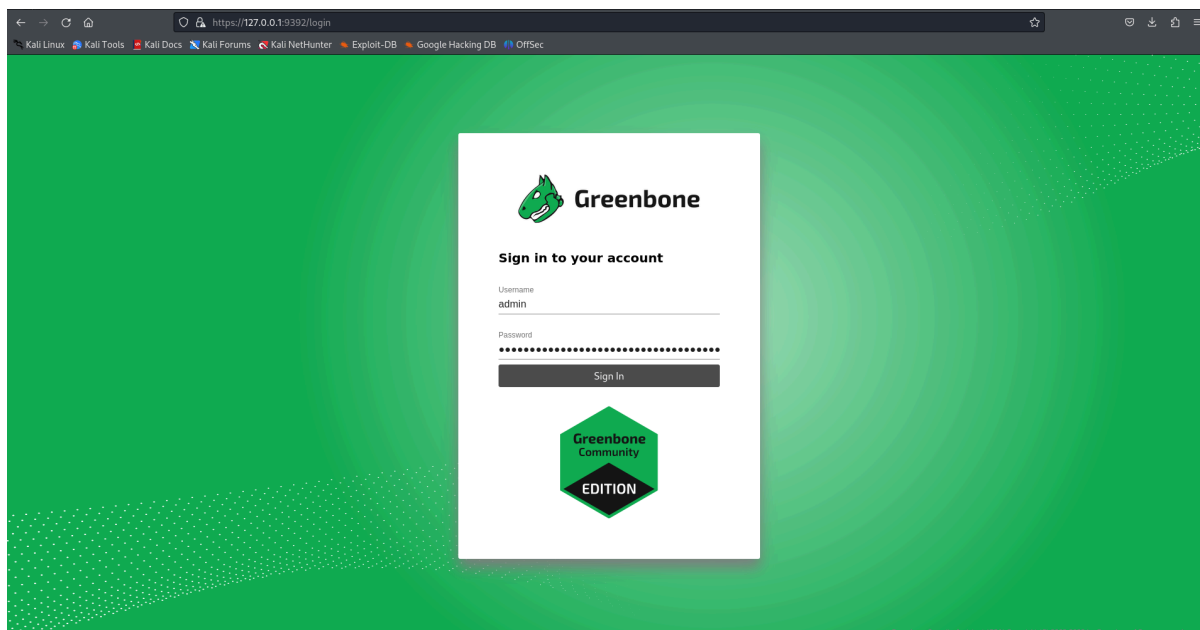
## Fonctionnement

OpenVAS fonctionne en envoyant des sondes aux cibles spécifiées et en analysant les réponses pour identifier les vulnérabilités connues. Il compare les résultats à une base de données de vulnérabilités régulièrement mise à jour, comprenant des milliers de tests de vulnérabilités (NVTs - Network Vulnerability Tests). Les résultats du scan sont ensuite analysés et présentés sous forme de rapports détaillés, permettant aux administrateurs de prioriser les actions correctives.

## Guide d'utilisation détaillé

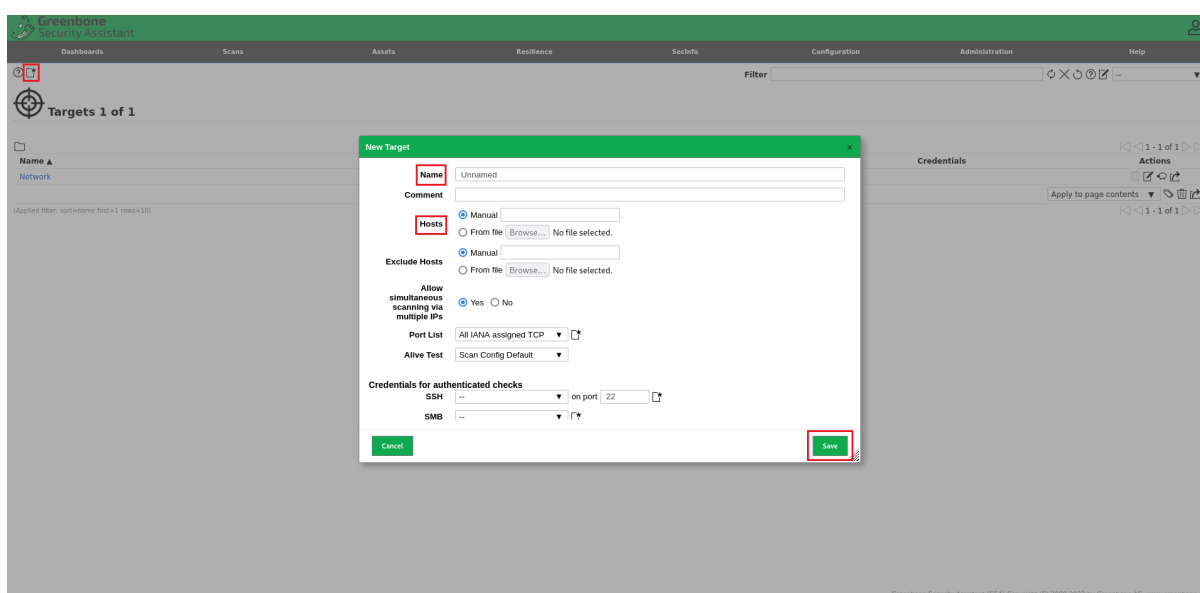
### 1. Lancement de l'interface web :

- Ouvrez un navigateur web et entrez l'URL de l'interface OpenVAS (généralement <https://127.0.0.1:9392>).
- Connectez-vous avec vos identifiants administratifs fournis lors de l'installation d'OpenVAS.



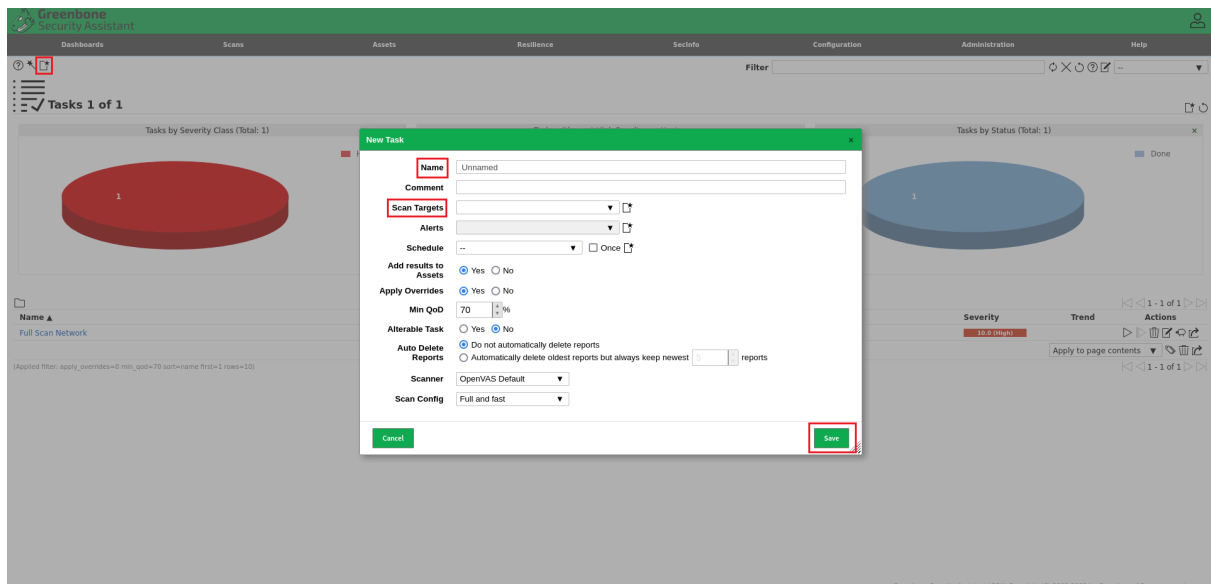
## 2. Configuration d'un nouveau scan :

- Allez dans la section "Targets" (Cibles).
- Cliquez sur "New Target" (Nouvelle cible).
- Donnez un nom à votre cible (par exemple, "Serveur Web Production").
- Indiquez l'adresse IP ou le sous-réseau à scanner (par exemple, 192.168.1.100-150 ou 192.168.1.0/24).
- Configurez d'autres paramètres optionnels comme les exclusions de scan (ports, répertoires, etc.).



### 3. Création d'une tâche (Task) :

- Allez dans la section "Tasks" (Tâches).
- Cliquez sur "New Task" (Nouvelle tâche).
- Donnez un nom à votre tâche (par exemple, "Scan complet du réseau").
- Sélectionnez la cible que vous venez de créer.
- Choisissez un profil de scan adapté à vos besoins :
  - "Full and fast" : Pour un scan rapide et complet.
  - "Host Discovery" : Pour découvrir les hôtes actifs sur le réseau.
  - "Web Application Tests" : Pour cibler les vulnérabilités spécifiques aux applications web.
- Pour un scan global classique, choisissez "Full and fast".



### 4. Exécution du scan :

- Sélectionnez votre tâche et cliquez sur "Start" (Démarrer).
- Le scan commence et vous pouvez suivre sa progression en temps réel.

### 5. Analyse des résultats :

- Une fois le scan terminé, accédez à la section "Reports" (Rapports).
- Sélectionnez votre scan pour voir les résultats détaillés. Vous pourrez ici consulter les différentes informations récupérées par le scan (hôtes, ports, applications, etc.).
- Les rapports incluent des détails sur les vulnérabilités détectées, classées par gravité (de "Log" à "Critique").

- Cliquez sur le bouton en haut à gauche pour télécharger le rapport au format PDF.

Compose Content for Scan Report

Results Filter

Include

☒ Notes
 ☒ Overrides
 ☒ TLS Certificates

Report Format

PDF ▼

☐ Store as default

Cancel

OK

- Consultez le rapport généré pour identifier les vulnérabilités détectées. Les rapports peuvent inclure des informations sur les correctifs disponibles et les mesures de mitigation.

## Explications supplémentaires sur les rapports OpenVAS

OpenVAS génère des rapports détaillés qui sont essentiels pour comprendre les vulnérabilités découvertes et pour planifier les actions correctives. Chaque rapport inclut les sections suivantes :

- **Résumé exécutif** : Une vue d'ensemble des résultats du scan, mettant en évidence les vulnérabilités critiques et les actions recommandées.
- **Détails des vulnérabilités** : Une liste des vulnérabilités trouvées, avec des descriptions détaillées, des scores de gravité (souvent basés sur le CVSS -

Common Vulnerability Scoring System), et des recommandations de remédiation.

- **Informations sur les hôtes** : Détails sur les hôtes scannés, y compris les adresses IP, les ports ouverts, les services détectés, les systèmes d'exploitation, et les versions logicielles.
- **Mesures correctives** : Conseils spécifiques pour corriger les vulnérabilités, y compris les liens vers les mises à jour de sécurité, les correctifs, et les configurations recommandées.

Ces rapports sont cruciaux pour les équipes de sécurité car ils fournissent une feuille de route claire pour améliorer la sécurité du réseau et des systèmes scannés.

## 2. Zaproxy

### Présentation

Zaproxy (Zed Attack Proxy), également connu sous le nom de ZAP, est un outil open-source de référence pour auditer la sécurité des applications web. Développé par l'OWASP (Open Web Application Security Project), ZAP est devenu un standard incontournable pour les professionnels de la cybersécurité. Il permet de détecter et d'analyser les vulnérabilités présentes dans les applications web, aidant ainsi les entreprises à protéger leurs services en ligne contre les attaques.

### Cas d'usage de Zaproxy :

- **Tests de pénétration d'applications web** : ZAP permet de simuler des attaques réalistes pour évaluer la résistance d'une application web face aux menaces courantes.
- **Développement sécurisé** : Les développeurs peuvent utiliser ZAP tout au long du cycle de développement pour identifier et corriger les vulnérabilités au fur et à mesure.
- **Audits de sécurité réguliers** : ZAP permet de vérifier périodiquement la sécurité d'une application web et de s'assurer qu'elle reste protégée contre les nouvelles menaces.
- **Évaluation de la conformité** : ZAP aide à vérifier si une application web respecte les normes de sécurité applicables (OWASP Top 10, PCI DSS, etc.).

### Zaproxy : Scans Externes pour Applications Web

Zaproxy est principalement utilisé pour réaliser des **scans externes** d'applications web, c'est-à-dire qu'il analyse l'application depuis l'extérieur, comme le ferait un attaquant potentiel. Ce type de scan permet de :



- **Identifier les vulnérabilités exposées sur Internet** : ZAP détecte les failles accessibles depuis l'extérieur, telles que les injections SQL, les failles XSS, les problèmes d'authentification, etc.
- **Évaluer la surface d'attaque** : ZAP cartographie l'application web et identifie les points d'entrée potentiels pour les attaquants.
- **Tester la robustesse des défenses** : ZAP simule des attaques pour vérifier si les mécanismes de sécurité de l'application sont efficaces.


En effectuant des scans externes avec Zaproxy, vous pouvez aider vos clients à identifier les vulnérabilités de leurs applications web avant qu'elles ne soient exploitées, et leur fournir des recommandations concrètes pour renforcer leur sécurité.

## Fonctionnement


ZAP fonctionne en interceptant et analysant le trafic entre votre navigateur et l'application web cible. Il vous permet de manipuler les requêtes et les réponses, de tester différentes attaques (injections SQL, XSS, etc.), et d'identifier les vulnérabilités présentes dans l'application.

## Guide d'utilisation détaillé

1. **Lancement de ZAP** : Ouvrez ZAP depuis votre menu d'applications ou en ligne de commande.
2. **Scan** :
  - Cliquez sur "Automated Scan" (Scan automatisé) directement affiché à l'ouverture de ZAP.
  - Entrez l'URL de l'application web que vous souhaitez scanner.
  - Cliquez ensuite sur "Attack" (Attaquer).



# Automated Scan



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.  
Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:  Select...

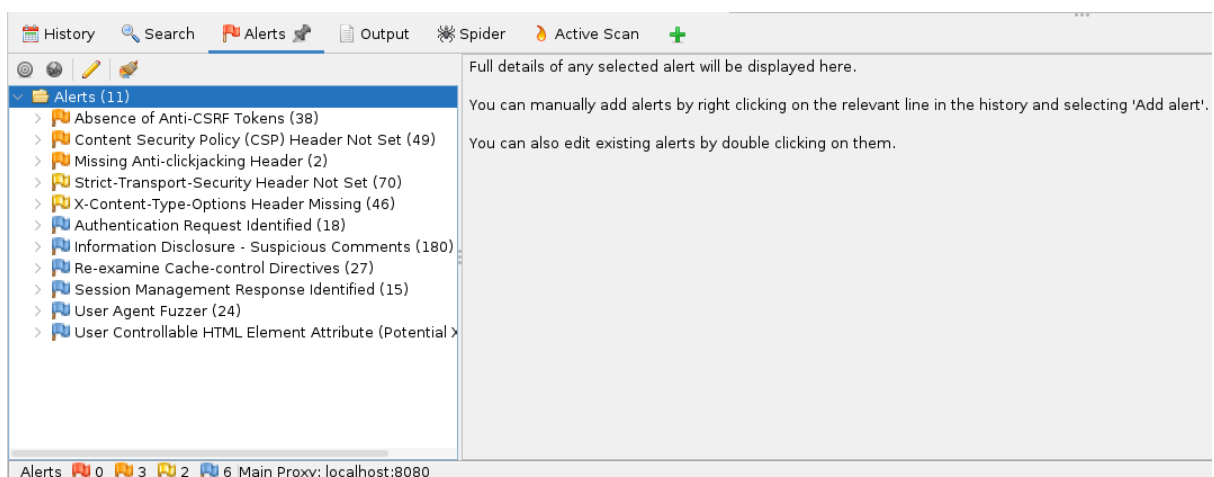
Use traditional spider: ☒

Use ajax spider: If Modern with Firefox Headless

Attack
Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

- Le scan automatique commence et ZAP analyse la cible pour identifier les vulnérabilités.
- Attendez la fin du scan puis analysez les résultats pour identifier les vulnérabilités.
- Les résultats sont affichés dans l'onglet "Alerts" (Alertes) à gauche de l'écran.



- Les vulnérabilités sont classées par gravité, avec des descriptions détaillées et des recommandations.

### 3. Génération de rapports :

- Allez dans la section "Report" en haut à gauche de la fenêtre et sélectionnez "Generate Report" (Générer un rapport).
- Choisissez le format du rapport (HTML, XML, JSON, etc.).
- Générez un rapport détaillé des vulnérabilités identifiées.

# ZAP Scanning Report

Generated with  ZAP on Wed 5 Jun 2024, at 12:32:47

ZAP Version: 2.15.0

ZAP is supported by the [Crash Override Open Source Fellowship](#)

## Contents

- [About this report](#)
  - [Report parameters](#)
- [Summaries](#)
  - [Alert counts by risk and confidence](#)
  - [Alert counts by site and risk](#)
  - [Alert counts by alert type](#)
- [Alerts](#)
  - [Risk=High, Confidence=High \(1\)](#)
  - [Risk=Medium, Confidence=High \(6\)](#)
  - [Risk=Medium, Confidence=Medium \(3\)](#)

## Explications supplémentaires sur les rapports Zaproxy

Les rapports générés par ZAP sont conçus pour être compréhensibles et actionnables, même pour ceux qui ne sont pas experts en sécurité. Voici quelques-unes des sections clés que vous trouverez dans un rapport ZAP :

- **Vue d'ensemble** : Une synthèse des résultats, y compris le nombre total de vulnérabilités trouvées et leur répartition par gravité.
- **Détails des vulnérabilités** : Chaque vulnérabilité est décrite en détail, avec des informations sur la nature de la vulnérabilité, comment elle peut être exploitée et les impacts potentiels.
- **Recommandations** : Conseils spécifiques pour corriger chaque vulnérabilité, y compris des liens vers des ressources supplémentaires ou des correctifs.
- **Logs de scan** : Un enregistrement détaillé des activités de scan, utile pour comprendre exactement comment et quand les vulnérabilités ont été détectées.

Les rapports ZAP sont essentiels pour les équipes de développement et de sécurité, car ils fournissent une base solide pour améliorer la sécurité des applications web.

### 3. Wifite

#### Présentation

Wifite est un outil d'audit de sécurité open-source conçu pour évaluer la robustesse des réseaux Wi-Fi. Il automatise le processus de test en simulant différentes attaques, permettant ainsi d'identifier les points faibles et les vulnérabilités potentielles de l'infrastructure Wi-Fi interne d'une entreprise.

#### Cas d'usage de Wifite :

- **Audits de sécurité Wi-Fi** : Évaluer la sécurité des réseaux Wi-Fi internes en testant la résistance des protocoles de sécurité (WEP, WPA/WPA2) et en identifiant les points d'accès mal configurés.
- **Tests de pénétration** : Simuler des attaques réalistes pour évaluer la capacité du réseau Wi-Fi à résister aux intrusions et identifier les vulnérabilités exploitables.
- **Détection de points d'accès non autorisés** : Découvrir les points d'accès non autorisés (rogue AP) qui pourraient être installés par des employés malveillants ou des personnes non autorisées.
- **Vérification de la configuration** : S'assurer que les paramètres de sécurité des réseaux Wi-Fi sont correctement configurés et conformes aux meilleures pratiques (chiffrement fort, mots de passe complexes, etc.).
- **Renforcement de la sécurité Wi-Fi** : Identifier les vulnérabilités et les faiblesses du réseau Wi-Fi pour mettre en place des mesures correctives et renforcer la sécurité globale.

**Important** : L'utilisation de Wifite doit être effectuée dans un cadre légal et éthique, avec l'autorisation préalable des propriétaires des réseaux Wi-Fi testés. Il est essentiel de respecter les lois et les réglementations en vigueur concernant la sécurité informatique.

#### Fonctionnement

Wifite fonctionne en lançant des attaques automatisées sur les réseaux Wi-Fi détectés pour tester leur sécurité. Il utilise des techniques de cracking bien connues pour tenter de compromettre les réseaux, offrant ainsi un aperçu des vulnérabilités potentielles. Wifite est capable de cibler différents types de sécurité Wi-Fi, notamment :

- **WEP** : Un protocole de sécurité obsolète et faible, facilement crackable par Wifite.
- **WPA/WPA2** : Protocoles plus robustes, mais Wifite peut utiliser des attaques par dictionnaire ou par force brute pour tenter de trouver la clé de sécurité.
- **WPS** : Une fonctionnalité de certains routeurs Wi-Fi qui peut être exploitée par Wifite pour obtenir la clé de sécurité rapidement.

## Guide d'utilisation détaillé

### 1. Lancement de Wifite :

- Ouvrez un terminal et lancez Wifite avec la commande `sudo wifite`.

### 2. Sélection des réseaux cibles :

- Wifite scanne les réseaux Wi-Fi à proximité et affiche une liste des réseaux détectés, avec des détails comme le nom (SSID), le canal, la puissance du signal, et le type de sécurité.
- Sélectionnez les réseaux cibles à auditer en entrant leur numéro dans la liste.

### 3. Lancement des attaques :

- Wifite automatise les attaques sur les réseaux sélectionnés. Il choisira les attaques appropriées en fonction du type de sécurité de chaque réseau.
- Patientez pendant que Wifite réalise les tests. Le processus peut prendre du temps, en fonction de la complexité des attaques et de la robustesse des réseaux cibles.

### 4. Analyse des résultats :

- Wifite affiche les résultats des attaques dans le terminal.
- Si une attaque réussit, Wifite affichera la clé de sécurité compromise.
- Analysez les résultats pour identifier les vulnérabilités des réseaux Wi-Fi. Par exemple, si Wifite a réussi à cracker une clé WEP, cela indique que le réseau est très peu sécurisé.

## Explications supplémentaires sur les attaques Wifite

- **Attaques WEP** : Wifite utilise des techniques comme le FMS (Fluhrer, Mantin, and Shamir) et le KoreK pour exploiter les faiblesses du protocole WEP et récupérer la clé de sécurité.
- **Attaques WPA/WPA2** : Wifite capture les handshakes WPA (échange de messages entre le client et le point d'accès) et tente de les déchiffrer en utilisant des attaques par dictionnaire (test de mots de passe courants) ou par force brute (test de toutes les combinaisons possibles).

- **Attaques WPS** : Wifite exploite les vulnérabilités du WPS (Wi-Fi Protected Setup) pour obtenir la clé de sécurité. Il utilise des techniques comme le Pixie-Dust et le Reaver pour deviner le PIN WPS, qui permet ensuite de récupérer la clé WPA/WPA2.

## 4. ScubaGear

### Présentation

ScubaGear est un outil d'audit de sécurité open-source spécialement conçu pour les environnements Office 365. Il permet d'analyser en profondeur les configurations, les permissions et les activités au sein de votre environnement Microsoft cloud, afin de détecter d'éventuelles failles de sécurité et de vous fournir des recommandations pour les corriger.

### Cas d'usage de ScubaGear :

- **Audits de sécurité Office 365** : Évaluation complète de la configuration de sécurité d'Office 365, y compris les paramètres de sécurité, les autorisations d'accès et les règles de conformité.
- **Détection des risques liés aux accès** : Identification des comptes disposant de privilèges excessifs, des boîtes aux lettres partagées non sécurisées et des délégations de permissions dangereuses.
- **Surveillance des activités suspectes** : Analyse des journaux d'activité pour détecter les comportements anormaux, les tentatives de connexion échouées, l'envoi massif de courriels et autres activités potentiellement malveillantes.
- **Vérification de la conformité** : Évaluation de la conformité d'Office 365 aux réglementations internes et externes (RGPD, HIPAA, etc.) ainsi qu'aux bonnes pratiques de sécurité.
- **Durcissement de la sécurité Office 365** : Mise en œuvre des recommandations fournies par ScubaGear pour renforcer la sécurité de votre environnement Office 365 et protéger vos données sensibles.

En utilisant cet outil, vous pouvez obtenir une vision claire de la sécurité d'un environnement Office 365, identifier les zones à risque et prendre des mesures proactives pour protéger les données et les utilisateurs.

### Fonctionnement

ScubaGear se connecte à votre environnement Office 365 en utilisant les API Microsoft Graph et analyse les données pour détecter les configurations non sécurisées, les accès excessifs, les activités suspectes, et les problèmes de conformité.

## Guide d'utilisation détaillé

### 1. Connexion à Office365 :

- Lancez le script fourni (via une invite de commande PowerShell en administrateur).
- Connectez-vous avec vos identifiants administrateurs Office365.
- L'audit se fera automatiquement et générera un rapport HTML détaillé.

Voici la commande à réaliser dans le dossier où se trouve le script :

```
python .\scuba_gear_script.py
```

### 2. Analyse des résultats :

- Consultez le rapport HTML généré par ScubaGear.
- Le rapport contient des informations détaillées sur les configurations de sécurité, les permissions, les activités suspectes, et les problèmes de conformité.
- Chaque problème est accompagné d'une description, d'un niveau de risque, et de recommandations pour le corriger.



Secure Cloud Business  
Applications (SCuBA)      Baseline  
Documents

Light Mode



## SCuBA M365 Security Baseline Conformance Reports

Tenant Display Name	Tenant Domain Name	Tenant ID	Report Date
			05/27/2024 10:01:26 Paris, Madrid (heure d'été)

Baseline Conformance Reports	Details			
<a href="#">Azure Active Directory</a>	4 tests passed	4 warnings	18 tests failed	4 manual checks needed
<a href="#">Microsoft 365 Defender</a>	0 tests passed	4 warnings	7 tests failed	5 manual checks needed 4 errors
<a href="#">Exchange Online</a>	6 tests passed	2 warnings	6 tests failed	23 manual checks needed
<a href="#">SharePoint Online</a>	2 tests passed		8 tests failed	1 manual check needed
<a href="#">Microsoft Teams</a>	5 tests passed	6 warnings	4 tests failed	6 manual checks needed

## Explications supplémentaires sur les audits ScubaGear

ScubaGear vérifie un large éventail de paramètres et de configurations dans Office 365, notamment :

- **Configurations de sécurité** : Activation de l'authentification multifacteur (MFA), configuration des politiques de mot de passe, restrictions sur les connexions à partir de pays étrangers, contrôles d'accès conditionnel.
- **Permissions et accès** : Rôles d'administrateur excessifs, permissions déléguées non sécurisées, accès aux boîtes aux lettres partagées.
- **Activités suspectes** : Tentatives de connexion échouées, activité de messagerie inhabituelle (envoi massif de mails, etc.), accès à des données sensibles par des utilisateurs non autorisés.
- **Politiques de conformité** : Conformité aux politiques de conservation des données, respect des réglementations (RGPD, HIPAA, etc.).

## 5. Domain\_Audit

### Présentation

Active Directory (AD) est le cœur battant de nombreuses entreprises, gérant les identités, les accès et les ressources. Sa sécurité est primordiale. Domain\_Audit est votre outil de prédilection pour auditer en profondeur cet environnement critique. Il scrute minutieusement chaque recoin de l'AD, révélant les failles de sécurité et les mauvaises configurations qui pourraient être exploitées par des attaquants.

### Cas d'usage de Domain\_Audit :

- **Audits de sécurité** : Évaluez la posture de sécurité de l'AD, identifiez les dérives de configuration et les failles potentielles comme les problèmes d'accès SMB.
- **Évaluation de la conformité** : Vérifiez si la configuration de l'AD est conforme aux normes de sécurité (NIST, CIS, etc.) et aux réglementations spécifiques à votre secteur d'activité.

### Exemples Concrets d'Utilisation :

- **Détecter les comptes à privilèges excessifs** : Identifiez les utilisateurs ayant des droits d'administrateur local sur un grand nombre de machines, ce qui constitue un risque majeur en cas de compromission de leur compte.
- **Repérer les faiblesses liées aux mots de passe** : Trouvez les comptes utilisant des mots de passe faibles, vides ou jamais expirés, et recommandez des mesures pour renforcer la politique de mots de passe.



- **Identifier les ordinateurs vulnérables** : Repérez les machines obsolètes, non patchées ou mal configurées (par exemple, avec le protocole SMBv1 activé), qui sont des cibles privilégiées pour les attaquants.
- **Contrôler les délégations** : Vérifiez si des délégations de permissions inappropriées ont été accordées, ce qui pourrait permettre à des utilisateurs d'accéder à des ressources auxquelles ils ne devraient pas avoir accès.

Domain\_Audit vous aidera à identifier ces problèmes et bien d'autres, vous permettant de fournir à vos clients des recommandations concrètes pour renforcer la sécurité de leur Active Directory.

## Fonctionnement

Domain\_Audit passe au crible tous les éléments clés de votre Active Directory : utilisateurs, groupes, ordinateurs, stratégies de groupe (GPO) et bien plus encore. Il recherche activement les configurations non sécurisées, les comptes à privilèges excessifs, les mots de passe faibles ou expirés, les erreurs de configuration courantes, et d'autres faiblesses qui pourraient compromettre la sécurité de l'infrastructure.

## Guide d'Utilisation Détaillé

### 1. Exécution de l'audit :

- **Désactivez entièrement votre antivirus.**
- Ouvrez une invite de commande PowerShell **en tant qu'administrateur**.
- Placez-vous dans le répertoire où se trouve le script `domain_audit_script.py`.
- Exécutez la commande suivante, en remplaçant les informations entre `< >` par les valeurs appropriées :

```
python .\domain_audit_script.py <domaine> <utilisateur> <mot de passe>
<serveur>
```

Par exemple :

```
python .\domain_audit_script.py exemple.local Administrateur Password123
192.168.0.10
```

- L'audit se lancera automatiquement et les résultats seront enregistrés dans des fichiers texte.

### 2. Analyse des résultats :

- Une fois l'audit terminé, un dossier portant le nom du domaine audité et la date sera créé (par exemple, "exemple.local-2024-06-05").
- À l'intérieur de ce dossier, ouvrez le sous-dossier "findings".

checks	27/05/2024 09:41	Dossier de fichiers
data	27/05/2024 09:49	Dossier de fichiers
findings	27/05/2024 09:41	Dossier de fichiers

- Vous y trouverez des fichiers texte, chacun correspondant à une catégorie de vulnérabilité ou de mauvaise configuration. Par exemple :
  - **access\_localadmin\_smb.txt** : Liste des machines permettant l'accès administrateur via SMB (Server Message Block), un protocole réseau courant.
  - **computers\_inactive.txt** : Liste des ordinateurs inactifs depuis un certain temps, pouvant être des machines oubliées ou potentiellement compromises.
  - **administrators\_notin\_protectedusersgroup.txt** : Comptes administrateurs n'étant pas membres du groupe "Protected Users", qui offre une protection renforcée.
- Analysez attentivement chaque fichier pour comprendre les problèmes identifiés. Le contenu de chaque fichier vous fournira des détails sur les éléments concernés (noms d'utilisateurs, noms de machines, etc.).

Nom	Modifié le	Type	Taille
ADIDNS_authenticated_users.txt	27/05/2024 09:41	Document texte	1 Ko
administrators_delegation_flag.txt	27/05/2024 09:41	Document texte	1 Ko
administrators_notin_protectedusersgrou...	27/05/2024 09:41	Document texte	1 Ko
authenticated_users_can_join_domain.txt	27/05/2024 09:41	Document texte	1 Ko
computers_inactive.txt	27/05/2024 09:40	Document texte	3 Ko
computers_OS_EOL.txt	27/05/2024 09:40	Document texte	1 Ko
computers_part_of_highprivilegedgroups...	27/05/2024 09:41	Document texte	1 Ko
computers_W10_EOS.txt	27/05/2024 09:40	Document texte	1 Ko
laps_notenabled.txt	27/05/2024 09:40	Document texte	1 Ko
large_amount_of_administrators.txt	27/05/2024 09:39	Document texte	1 Ko
oldpassword_krbtgt.txt	27/05/2024 09:40	Document texte	1 Ko
oldpassword_privilegedusers.txt	27/05/2024 09:40	Document texte	1 Ko
passwordpolicy.txt	27/05/2024 09:40	Document texte	1 Ko
printspooler_domaincontrollers.txt	27/05/2024 09:41	Document texte	1 Ko
users_dontexpirepassword.txt	27/05/2024 09:40	Document texte	2 Ko
users_inactive.txt	27/05/2024 09:40	Document texte	3 Ko

## Interprétation des Résultats

Les fichiers texte de Domain\_Audit ne sont pas des rapports formels, mais des listes de résultats bruts. Il est essentiel de comprendre la signification de chaque fichier pour interpréter correctement les résultats :

- **Fichiers commençant par "access\_"** : Indiquent des problèmes de contrôle d'accès, comme des utilisateurs ayant des privilèges excessifs ou des partages de fichiers mal configurés.
- **Fichiers commençant par "computers\_"** : Concernent les problèmes liés aux ordinateurs, tels que les systèmes non patchés, les configurations SMB non sécurisées, ou les machines inactives.
- **Fichiers commençant par "administrators\_"** : Signalent les problèmes liés aux comptes administrateur, comme des mots de passe faibles ou l'absence de protection supplémentaire.
- **Autres fichiers** : Peuvent indiquer d'autres problèmes de configuration ou de sécurité spécifiques à Active Directory.

### Exemple d'Interprétation : access\_localadmin\_smb.txt

Si le fichier `access_localadmin_smb.txt` contient des entrées, cela signifie que certaines machines de l'Active Directory audité autorisent des connexions à distance avec des privilèges administrateur via le protocole SMB. Il s'agit d'un risque de sécurité important, car un attaquant qui parviendrait à compromettre un compte utilisateur standard pourrait potentiellement prendre le contrôle total de ces machines.

## Actions Correctives

Les actions à entreprendre dépendent de la nature des vulnérabilités identifiées. Voici quelques exemples d'actions correctives possibles :

- **Restreindre les accès administrateur** : Limitez les droits d'administration locale aux seuls utilisateurs qui en ont réellement besoin.
- **Appliquer des politiques de mots de passe forts** : Exigez des mots de passe complexes et longs, et mettez en place une politique de renouvellement régulier.
- **Activer l'authentification multifacteur (MFA)** : Renforcez la sécurité des comptes à privilèges élevés en exigeant une deuxième forme d'authentification.
- **Appliquer les correctifs de sécurité** : Maintenez les systèmes à jour avec les derniers correctifs de sécurité pour réduire les risques d'exploitation de vulnérabilités connues.
- **Mettre en place un système de gestion des privilèges** : Contrôlez et surveillez l'accès aux privilèges élevés pour minimiser les risques d'abus.

N'oubliez pas que chaque environnement Active Directory est unique. Il est crucial d'analyser les résultats de Domain\_Audit en tenant compte du contexte spécifique de votre client pour formuler des recommandations pertinentes et adaptées à ses besoins.

## **Conclusion**

Ce guide vous a présenté les bases pour utiliser efficacement cinq outils open-source puissants lors de vos audits de sécurité. En maîtrisant OpenVAS, Zaproxy, Wifite, ScubaGear et Domain\_Audit, vous serez en mesure d'offrir à vos clients une évaluation complète de leur sécurité informatique, couvrant aussi bien les réseaux, les applications web, le Wi-Fi, Office 365 qu'Active Directory.

Ces outils vous permettront de détecter un large éventail de vulnérabilités et de mauvaises configurations, vous donnant ainsi les clés pour protéger les systèmes et les données de vos clients. En présentant des rapports clairs et concis, assortis de recommandations concrètes, vous aiderez vos clients à comprendre les risques auxquels ils sont confrontés et à prendre les mesures nécessaires pour renforcer leur sécurité.

N'oubliez pas que la sécurité informatique est un processus continu. Des audits réguliers et l'utilisation d'outils adaptés sont essentiels pour maintenir un niveau de sécurité élevé et protéger vos clients contre les menaces en constante évolution.