

{{ client }}

{{ contract }}

{{ month|translate }} {{ year }}

Rapport de test d’intrusion

Note de confidentialité

Ce document contient des informations confidentielles. Il ne peut être diffusé ou transféré en dehors de votre organisation sans l’autorisation écrite d’une personne habilitée par AlgoSecure. Il ne peut être copié ou reproduit sous quelque forme que ce soit. AlgoSecure est un nom déposé.

Cycle éditorial

|  |  |  |
| --- | --- | --- |
| Nom | Rôle | Email |
| {{ owner.surname }} {{ owner.name }} | Auditeur, Rédacteur | {{ owner.email}} |
| {%tr for pentester in pentesters %} |  |  |
| {{ pentester.surname }} {{ pentester.name}} | Auditeur, Relecteur | {{ pentester.email }} |
| {%tr endfor %} |  |  |
| Hicham Ben Hassine | Approbateur | hicham.ben-hassine@algosecure.fr |

Contacts client

|  |  |  |
| --- | --- | --- |
| Nom | Téléphone | Email |
|  |  |  |

Contacts AlgoSecure

|  |  |  |
| --- | --- | --- |
| Nom | Téléphone | Email |
| Hicham Ben Hassine | 06 20 23 39 74 | hicham.ben-hassine@algosecure.fr |
| Antoine Breuillé | 06 38 04 87 78 | antoine.breuille@algosecure.fr |
| Julien Haug | 06 66 59 77 21 | julien.haug@algosecure.fr |
| Luc Maurice | 06 25 97 42 54 | luc.maurice@algosecure.fr |
| Diane Serra | 06 42 62 41 95 | diane.serra@algosecure.fr |

*Notre service commercial est joignable à* [*commercial@algosecure.fr*](mailto:commercial@algosecure.fr)*.*

*Notre support technique est joignable au* ***04 26 78 24 86****.*

Sommaire

[1. Introduction 2](#_Toc511999554)

[1.1. Présentation d’AlgoSecure 2](#_Toc511999555)

[1.2. Contexte de l’audit 2](#_Toc511999556)

[1.3. Structure de ce rapport 2](#_Toc511999557)

[2. Synthèse des résultats 2](#_Toc511999558)

[2.1. Niveau de sécurité global 2](#_Toc511999563)

[2.2. Menaces concrètes 2](#_Toc511999564)

[2.3. Défauts constatés 2](#_Toc511999565)

[2.4. Points forts 2](#_Toc511999566)

[2.5. Mauvaises pratiques 2](#_Toc511999567)

[2.6. Points de vigilance 2](#_Toc511999568)

[2.7. Conformité avec les recommandations AlgoSecure [si pertinent] 2](#_Toc511999569)

[2.8. Défauts corrigés [si pertinent] 2](#_Toc511999570)

[3. Tableau récapitulatif des vulnérabilités 2](#_Toc511999571)

[4. Tableau récapitulatif des actions correctives 2](#_Toc511999572)

[5. Détail des défauts et actions correctives 2](#_Toc511999573)

[6. Annexes 2](#_Toc511999574)

[6.1. Échelle de classification des vulnérabilités 2](#_Toc511999581)

[6.2. Notre démarche de tests d’intrusion 2](#_Toc511999582)

[6.3. Tests réalisés 2](#_Toc511999583)

[6.4. Services ouverts 2](#_Toc511999584)

[6.5. Glossaire 2](#_Toc511999585)

[6.6. Outils utilisés 2](#_Toc511999586)

# Introduction

## Présentation d’AlgoSecure

AlgoSecure est un cabinet lyonnais spécialisé dans la sécurité des systèmes d’information, créé en 2008 composée d’une équipe technique hautement qualifiée : membre du CLUSIR, participations aux OzSSI, FIC, formation OSSIR, challenge d’Ethical Hacking (Insomni’Hack, Hack In Paris, GreHack…).

Notre métier est d’accompagner nos clients sur tout type de projets, infrastructure ou applicatif afin d’améliorer leurs compétences SSI au travers de différents services : audits de sécurité, tests d’intrusion, AMOA, formations, guides de sécurisation, définition de PSSI (Politique de Sécurité du Système d’Information), détection d’intrusion, analyse de risques, supervision SSI…

Nous revendiquons notre indépendance vis-à-vis des éditeurs ou constructeurs. Nous intervenons en conseil et en délégation de personnel.

Depuis novembre 2020, nous sommes **Prestataire d'Audit de la Sécurité des Systèmes d'Information** (PASSI). Cette qualification délivrée par l'ANSSI atteste de nos compétences en tant qu'auditeurs, mais aussi du soin que nous apportons à la confidentialité des données sensibles auxquelles nous pouvons être amenés à avoir accès durant nos prestations chez des clients. En outre, cette qualification atteste de notre respect de la norme d'audits [ISO 19001](https://www.iso.org/fr/standard/70017.html). Nous avons obtenu cette qualification sur les portées **Test d'intrusion**, **Audit de configuration**, **Audit d'architecture** et **Audit organisationnel et physique**.

## Contexte de l’audit

La société {{ client }} a mandaté AlgoSecure pour évaluer la sécurité de son [Périmètre] face aux attaques. Le périmètre considéré pour l’audit est le suivant :

Réseau interne de la société {{ client }}

**Test d’intrusion Boite Noire**

Les menaces proviennent d’un attaquant ayant uniquement accès au périmètre, sans aucun privilège spécifique ou compte utilisateur. Ce type d’audit permet d’évaluer les **menaces engendrées par un attaquant extérieur à la société**.

**Test d’intrusion Boite Grise**

Les menaces proviennent d’un attaquant ayant **un compte du domaine**. Ce type d’audit permet d’évaluer les **menaces engendrées par un utilisateur standard, ou un attaquant externe ayant élevé ses privilèges** en tant qu’utilisateur standard.

L’audit s’est déroulé **du [Jour au jour mois année]** depuis le site de [Société] à [Ville], depuis le réseau [A.B.C.D/X]. Deux consultants ont travaillé sur cet audit pour une charge totale de **[Nombre] jours-hommes**.

L’audit mené est non-destructif : il ne vise ni à menacer l’intégrité des données en place, ni à menacer le bon fonctionnement des services (pas de déni de service, notamment).

## Réserves [si pertinent]

[En raison de la taille conséquente du réseau de la société et en accord avec les commanditaires de l’audit, nous nous sommes concentrés sur le réseau A.B.C.D/X.]

## Structure de ce rapport

Ce rapport débute par une **synthèse** dans laquelle sont décrits le niveau de sécurité global et les impacts métiers potentiels résultant des failles découvertes.

Une deuxième partie décrit les **scénarios d’attaque** qui peuvent être réellement mis en œuvre à l’aide des vulnérabilités identifiées.

Une troisième partie détaille chaque **défaut de sécurité** identifié, ainsi que les **actions correctives** que nous préconisons.

Afin de clarifier la lecture du présent rapport, un **glossaire** est disponible en annexe. S’y trouve aussi **l’échelle de classification des vulnérabilités** que nous utilisons (ANSSI). Enfin, dans le cadre de notre démarche de transparence, nous mettons également à votre disposition la **liste des outils et scripts éventuels** utilisés pour réaliser cet audit.

# Synthèse des résultats

## Niveau de sécurité global

Au vu des résultats de cet audit, effectué [Quand], le périmètre audité dans le contexte précisé présente un niveau de sécurité global [**CRITIQUE**, **insatisfaisant**, **perfectible**, **satisfaisant**].



**Critique Insatisfaisant Perfectible Satisfaisant**

Cette évaluation se base sur différents facteurs, tel que la gravité des défauts de sécurité constatés, les risques que présentent l’exploitation de ces défauts dans votre contexte, ainsi que l’expérience des auditeurs face à des périmètres similaires précédemment audités.

Nous répartissons les défauts de sécurité dans 4 catégories : la sécurité de l’Active Directory et des systèmes Microsoft de manière générale, la sécurité de l’infrastructure et des services standard, la sécurité des données, et la politique de sécurité constatée. Chaque critère est évalué sur une échelle de quatre niveaux (Satisfaisant, Perfectible, Insatisfaisant et Critique), synthétisée ci-dessous.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Active Directory** | **Infrastructure** | **Données** | **Politique** |  | **GLOBAL** |

Durant les [nombre] jours dévolus à l’audit, nous avons déterminé qu’un attaquant, qu’il soit en situation de « boîte noire » ou « boîte grise » sur le réseau interne était en mesure rapidement :

* d’**élever ses privilèges en administrateur** du domaine Active Directory ;
* d’**accéder à un grand nombre de données personnelles et de données métiers** ;
* d’**accéder aux documents d’autres utilisateurs** sur les partages de fichiers ;
* d’**exfiltrer des données** de manière discrète vers Internet.

[Synthèse ToDo]

AlgoSecure vous recommande d’effectuer un **contre-audit** après que tout ou partie des corrections aient été appliquées, afin de s’assurer que les risques contre lesquels vous souhaitez vous prémunir aient bien été éliminés et que d’autres vulnérabilités n’aient pas été introduites.

## Menaces concrètes

Le terme « attaquant » désigne une personne ne possédant pas de compte sur l’application. Le terme « utilisateur » désigne une personne connectée à l’application, c’est-à-dire soit un utilisateur légitime, soit un attaquant connecté à la place d’un utilisateur légitime.

|  |  |  |  |
| --- | --- | --- | --- |
| **Menaces concrètes** | | **Conditions initiales** | **Défauts** |
| **M1** | Première menace | Accès depuis Internet | **D1**, **D2**, **D3** |
| **M2** | Deuxième menace | Accès utilisateur | **D1**, **D2** |
| **M3** | Troisième menace | Accès administrateur | **D1** |

## Défauts constatés

Durant cet audit, {{ defects|count }} **défauts de sécurité** ont été identifiés :

|  |  |  |  |
| --- | --- | --- | --- |
| Critique : **{{ defects | selectattr('risk','equalto', 'Critical')|list|count }}** | Majeur : **{{ defects | selectattr('risk','equalto', 'Major')|list|count }}** | Important : **{{ defects | selectattr('risk','equalto', 'Important')|list|count }}** | Mineur : **{{ defects | selectattr('risk','equalto','Minor')|list|count }}** |

L’évaluation de leur criticité est basée sur l’échelle de classification des vulnérabilités proposée par l’ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information), fournie dans les annexes.

{%p if positive\_remarks | count is ge 1 %}

## Points forts

{%p for positive\_remark in positive\_remarks %}

* {{ positive\_remark }}

{%p endfor %}

{%p endif %}

{%p if negative\_remarks | count is ge 1 %}

## Mauvaises pratiques

{%p for negative\_remark in negative\_remarks %}

* {{ negative\_remark }}

{%p endfor %}

{%p endif %}

{%p if neutral\_remarks | count is ge 1 %}

## Points de vigilance

{%p for neutral\_remark in neutral\_remarks %}

* + {{ neutral\_remark }}

{%p endfor %}

{%p endif %}

## Conformité avec les recommandations AlgoSecure [si pertinent]

Le tableau ci-dessous détaille l’état de conformité de l’application vis-à-vis des recommandations de sécurité ayant pu être évaluées dans le cadre de cet audit. En effet, un audit de type test d’intrusion ne permet pas d’évaluer des recommandations d’ordre organisationnel.

|  |  |
| --- | --- |
| Première recommandation |  |
| Deuxième recommandation |  |
| Troisième recommandation |  |

## Défauts corrigés [si pertinent]

Les défauts suivants ont été trouvés lors d’un précédent audit du périmètre spécifié.

|  |  |
| --- | --- |
| Défaut ayant été corrigé | **Corrigé** |
| Défaut n’ayant pas été corrigé | **Non corrigé** |
| Défaut ayant été partiellement corrigé | **Insuffisant** |

# Scénarios d’exploitation

À partir des défauts de sécurité identifiés, nous avons construit desscénarios d’exploitation réalistes. Les défauts sont matérialisés par des bulles dont la couleur reflète la criticité. Les cadres verts représentent les objectifs principaux, et les cadres bleus les objectifs intermédiaires.

*[Insérer le scénario d’exploitation global]*

|  |  |  |  |
| --- | --- | --- | --- |
| **S1** | **Premier scénario** | *Exploitation* | *Impact* |
| **[Exploitation]** | **[Impact]** |
| **Conditions de départ :** [conditions]  **Objectif final :** [objectif] | | | |

*[Insérer ici le scénario d’exploitation partiel]*

Un **attaquant externe** effectue [actions] afin de **[objectif intermédiaire]** grâce à [défaut] (défaut **DX**). Ce faisant, il réussit à **[objectif final]**.

# Tableau récapitulatif des défauts de sécurité

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Libellé** | **Exploitation** | **Impact** | **Type** |
| **{%tr for x in defects|selectattr('risk','equalto', 'Critical') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Major') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Important') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate}} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Minor') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |

***Critère « Type »****: S = Socle, A = Application, D = Données, P = Politique de sécurité*

*Le détail de l’échelle de classification des défauts de sécurité est donné en Annexe.*

# Tableau récapitulatif des actions correctives

Le critère de mise en œuvre est donné à titre indicatif, en se basant sur notre expérience, mais ne reflète pas les particularités de votre environnement qui pourraient complexifier la tâche.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Libellé** | **Mise en œuvre** | **Gain en sécurité** |
| **{%tr for fix in fixes %}** |  |  |  |
| **A{{ fix.id }}** | {{ fix.title }} | **{% cellbg colors.fix[fix.execution] %}{{ fix.execution|translate }}** | **{% cellbg colors.fix[fix.gain] %}{{ fix.gain|translate }}** |
| **{%tr endfor %}** |  |  |  |

***Critère « Mise en œuvre »***

*Quick Win : paramétrage d’un composant, protection d’une saisie d’une application*

*Modérée : changements de code restreints, mise en place d’une solution*

*Envergure : changements conséquents dans le code ou l’architecture de la solution*

# Tableau synthétique des résultats de l’audit

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **{%tr for x in defects|selectattr('risk','equalto', 'Critical') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | *Risque*  {{ x.risk|translate }} | *Exploitation*  {{ x.ease|translate }} | *Impact*  {{ x.impact|translate }} |
| **{%tr for fix in x.fixes %}** |  | |  |  |
| **A{{ fix.id }}** | {{ fix.title }} | | *Mise en œuvre*  {{ fix.execution|translate }} | *Gain en sécurité*  {{ fix.gain|translate }} |
| **{%tr endfor %}** |  | |  |  |
| **{%tr endfor %}** |  | |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Major') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | *Risque*  {{ x.risk|translate }} | *Exploitation*  {{ x.ease|translate }} | *Impact*  {{ x.impact|translate }} |
| **{%tr for fix in x.fixes %}** |  | |  |  |
| **A{{ fix.id }}** | {{ fix.title }} | | *Mise en œuvre*  {{ fix.execution|translate }} | *Gain en sécurité*  {{ fix.gain|translate }} |
| **{%tr endfor %}** |  | |  |  |
| **{%tr endfor %}** |  | |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Important') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | *Risque*  {{ x.risk|translate }} | *Exploitation*  {{ x.ease|translate }} | *Impact*  {{ x.impact|translate }} |
| **{%tr for fix in x.fixes %}** |  | |  |  |
| **A{{ fix.id }}** | {{ fix.title }} | | *Mise en œuvre*  {{ fix.execution|translate }} | *Gain en sécurité*  {{ fix.gain|translate }} |
| **{%tr endfor %}** |  | |  |  |
| **{%tr endfor %}** |  | |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Minor') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | *Risque*  {{ x.risk|translate }} | *Exploitation*  {{ x.ease|translate }} | *Impact*  {{ x.impact|translate }} |
| **{%tr for fix in x.fixes %}** |  | |  |  |
| **A{{ fix.id }}** | {{ fix.title }} | | *Mise en œuvre*  {{ fix.execution|translate }} | *Gain en sécurité*  {{ fix.gain|translate }} |
| **{%tr endfor %}** |  | |  |  |
| **{%tr endfor %}** |  | |  |  |

***Critère « Mise en œuvre »***

*Quick Win : paramétrage d’un composant, protection d’une saisie d’une application*

*Modérée : changements de code restreints, mise en place d’une solution*

*Envergure : changements conséquents dans le code ou l’architecture de la solution*

# Détail des défauts et actions correctives{% for x in defects|selectattr('risk','equalto', 'Critical') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

TODO {{ x.redactor }}

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Major') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

TODO {{ x.redactor }}

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Important') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

TODO {{ x.redactor }}

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Minor') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

TODO {{ x.redactor }}

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}

# Annexes

## Tableau de [quelque chose]

Le tableau suivant contient...

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Colonne 1 | Colonne 2 | Colonne 3 | Colonne 4 | Colonne 5 |
|  |  |  |  |  |
|  |  |  |  |  |

## Partages SMB accessibles aux anonymes

|  |  |  |  |
| --- | --- | --- | --- |
| Adresse IP | Nom d’hôte | Partages | Droits |
| IP | Nom d’hôte | Partage | Lecture/Écriture |
| IP | Nom d’hôte | Partage1  Partage2  Partage3 | Lecture seule  Lecture/Écriture  Lecture seule |

## Échelle de classification des vulnérabilités

Les vulnérabilités identifiées sont évaluées suivant l’échelle standard de classification des vulnérabilités proposée par l’ANSSI, l’Agence Nationale de la Sécurité des Systèmes d’Information, à destination des Prestataires-Auditeurs de la Sécurité des Systèmes d’Information (PASSI).

Elles sont classées en fonction du risque qu’elles font peser sur le système d’information, c'est-à-dire en fonction de l’impact de la vulnérabilité sur le système d’information et de sa difficulté d’exploitation, et ce qu’elles soient d’origine technique ou organisationnelle

Exploitation :

* **Facile :** exploitation triviale, sans outil particulier ;
* **Modérée :** exploitation nécessitant des techniques simples et des outils publics ;
* **Difficile :** exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d’information et le développement d’outils simples ;
* **Très difficile :** exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d’information et le développement d’outils spécifiques et ciblés.

Impact :

* **Mineur :** pas de conséquence directe sur la sécurité du système d’information audité ;
* **Important :** conséquences isolées sur des points précis du système d’information audité ;
* **Majeur :** conséquences restreintes sur une partie du système d’information audité ;
* **Critique :** conséquences généralisées sur l’ensemble du système d'information audité.

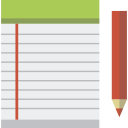
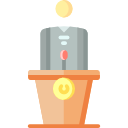
Risque résultant :

* **Mineur :** faible risque pouvant nécessiter une correction ;
* **Important :** risque modéré nécessitant une correction à moyen terme ;
* **Majeur :** risque majeur nécessitant une correction à court terme ;
* **Critique :** risque critique nécessitant une correction immédiate ou un arrêt immédiat.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **↓ Impact Exploit. →** | **Très difficile** | **Difficile** | **Modérée** | **Facile** |
| **Mineur** | Mineur | Mineur | Important | Majeur |
| **Important** | Mineur | Important | Important | Majeur |
| **Majeur** | Important | Majeur | Majeur | Critique |
| **Critique** | Important | Majeur | Critique | Critique |

## Notre démarche de tests d’intrusion

Notre approche des tests d’intrusion est basée sur notre expérience ainsi que sur les recommandations de l’OWASP et l’OSSTMM. Elle se décompose en plusieurs étapes.



Cette démarche correspond aux bonnes pratiques internationales et a pour objectif la réalisation d’un audit dans les règles de l’art et l’optimisation du temps imparti. Par ailleurs, nous respectons le périmètre que vous nous imposez, que cela soit en termes de cible, de plage temporelle, ou de type d’attaques (pas d’attaque par déni de service, par exemple).

Nos audits sont non-destructifs : nous n’effectuons **pas de tests visant à stopper l’activité des services type déni de service**. En outre, lors de la réunion de lancement, nous vérifions avec vous l’environnement du système audité (production ou pré-production) et la possibilité ou non d’ajouter, modifier ou supprimer des données.

## Tests réalisés

Cette liste mentionne tous les tests que nous réalisons habituellement, y compris les tests qui n’ont pas permis de mettre à jour des vulnérabilités, ou les tests non-applicables dans votre cas. Si vous nous avez demandé de ne pas effectuer certains tests, ceux-ci sont barrés.

**Audit Interne LAN et Active Directory**

* Identification et énumération des réseaux, machines et services
* Identification des partages réseau et de leurs droits d’accès
* Identification des protocoles obsolètes (SMBv1, LLMNR & NBT-NS, WDigest...)
* Identification de la politique de sécurité (contraintes de mots de passe, sécurité des postes...)
* Identification des chemins d’attaques de l’Active Directory
* Identification des caméras de sécurité non protégées
* Test des failles Exchange (PrivExchange, MIC-Remove)
* Test des failles Active Directory (BlueKeep, DCSync, EternalBlue, Kerberoasting…)
* Tests sur la sécurité des postes (configuration de l’antivirus, élévation de privilèges...)
* Test des bonnes pratiques Microsoft (LAPS, administration n-tiers...)
* Tests d’identifiants connus sur les interfaces d’administration
* Tests de relai d’identifiants
* Tests d’exfiltration de données vers Internet (contournement de proxy, DNS tunneling…)

## Glossaire

**Bruteforce :** désigne une attaque grâce à laquelle un attaquant va envoyer un grand nombre de requêtes automatisées au serveur, notamment dans le but de tenter de découvrir des identifiants de comptes utilisateurs valides en utilisant une liste de mots de passe connus ou triviaux.

**Cross-Site Scripting (XSS) :** une faille XSS permet à un attaquant malveillant de faire exécuter du code Javascript sur le navigateur de sa victime en tirant parti de la faiblesse de protection d’un champ d’une application. Utilisation courante : récupération de cookie.

**Déni de service (DoS) :** attaque consistant à saturer un équipement informatique de connexions, générées par un programme, jusqu’à ce que cet équipement ne puisse plus répondre aux demandes légitimes des clients. Lorsque cette attaque provient de plusieurs endroits dans le monde (généralement orchestrée par un seul attaquant), on parle de DDoS (*Distributed DoS*).

**Exploit :** un exploit est un code permettant d’exploiter un défaut de sécurité d’un équipement informatique, qui peut être rendu public (le plus souvent) ou vendu, en fonction de la criticité de la vulnérabilité exploité et de la facilité d’utilisation de l’exploit.

**Injection SQL (SQLi) :** une injection SQL tire parti de la faiblesse de protection d’un champ d’une application afin d’interagir directement avec la base de données dans le but de lui faire effectuer des actions illégitimes. Utilisation courante : bypass d’authentification.

**Man-in-the-Middle (MitM)** : dans une situation de Man-in-the-Middle, ou d’homme du milieu, un attaquant réussit à s’interposer entre l’ordinateur de sa victime et Internet (ou un hôte du réseau interne). Il est alors en mesure de lire, modifier, puis retransmettre le trafic entre un utilisateur et un serveur. Cette situation se produit généralement en situation de mobilité, lorsque l’utilisateur se connecte à un point d’accès WiFi public, qu’il soit « bien » sécurisé ou non.

## Outils utilisés

|  |  |
| --- | --- |
| ADRecon | Recensement des objets de l’Active Directory |
| BloodHound | Utilitaire de mappage des entités de l’Active Directory |
| CrackMapExec | Exécution de commandes à distance sur des hôtes Windows |
| Empire | Boîte à outils d’exploits et d’attaques orientées Windows |
| Hashcat | Crack de mots de passe (version hashée -> version en clair) |
| Impacket | Outils Python pour l’audit offensif en milieu Windows |
| John the Ripper | Crack de mots de passe (version hashée -> version en clair) |
| Mimikatz | Outil pour retrouver le mot de passe des utilisateurs en mémoire |
| Metasploit | Boîte à outils d’exploits et d’attaques tous OS |
| nmap | Scanneur de ports et services |
| PhantomJS | Navigateur Internet sans affichage, pour prendre des captures d’écran |
| Responder | Capture de séquence d’authentification Windows |
| smbmap | Utilitaire de listing des partages de fichiers SMB |
| unicornscan | Scanneur de ports et services |

**AlgoSecure**

57 boulevard Marius Vivier Merle

69003 Lyon

Notre site Internet : [www.algosecure.fr](http://www.algosecure.fr)

Retrouvez-nous sur Twitter : [@algosecure](https://twitter.com/AlgoSecure)