AIRS INFORMATIQUE

Toute l'informatique au service des professionnels.

Pentest - Test d'intrusion

Qu'est-ce qu'un pentest applicatif ?

Le pentest, également appelé test d'intrusion en français, est une technique de piratage éthique consistant à tester la vulnérabilité d'un système informatique, d'une application ou d'un site web en détectant les failles susceptibles d'être exploitées par un hacker ou un logiciel malveillant.

Réalisé par notre Pentester il a pour objectif primordial :

⇒ d'évaluer efficacement le risque associé à un système d'information

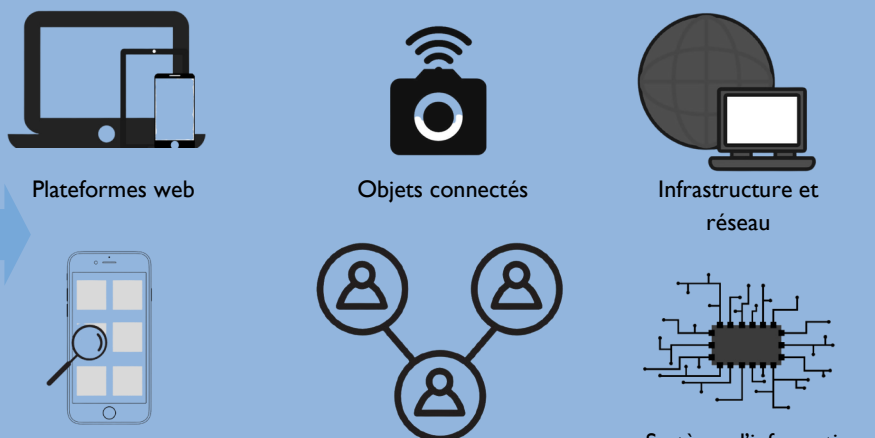
⇒ d'identifier des pistes pour réduire les vulnérabilités présentes

Grâce à cette approche, le Test d'intrusion permet de déterminer un maximum de vulnérabilités susceptibles d'être exploitées et ainsi améliorer la cybersécurité.

Le test d'intrusion n'est pas un audit de sécurité ! Si ce dernier s'effectue en suivant des normes ou un référentiel bien le pentest quant à lui est encadré par une lettre de mission dont vous déterminez le périmètre.

Définition du champ d'investigation

Approche complète ou ciblée



Typologie des types de test d'intrusion

Boite noire

Le pentester n'a aucune connaissance préalable de votre environnement. Il s'introduit dans votre système par n'importe quels moyens et subterfuges tout comme le ferait un hacker décidé à violer votre intégrité

Boite grise

Le Pentester se positionne en tant que collaborateur ayant un accès interne ou un hacker ayant réussi à avoir accès à un compte utilisateur ou à une adresse IP. Cela consiste à s'introduire dans le système d'information en disposant d'un nombre limité d'informations.

Méthode la plus utilisée car elle est souvent la plus réaliste

Boite blanche

Le Pentester a accès à la totalité des informations sur le système. Le consultant travaille en collaboration avec les équipes techniques afin de détecter un maximum de vulnérabilités.

Les étapes du Pentest

1 - Phase de reconnaissance	Collecte d'informations
2 - Phase de cartographie et d'énumération	Inventorier et cartographier
3 - Phase de recherche de vulnérabilités	Analyser les faiblesses
4 - Exploitation	Mise en application du travail effectué
5 - Elévations de privilèges	Se substituer à l'administrateur du système
6 - Maintien d'accès	Obtenir de nouveaux privilèges et les maintenir
7 - Propagation/déplacements latéraux	Etendre la compromission d'un poste
8 - Cleanup	Nettoyage des traces de l'auditeur sur le SI
9 - Présentation du rapport	Proposer des correctifs adaptés

Reporting

Présentation globale :

-Rappel du contexte et la lettre de mission du pentest.

-Présentation de la situation globale sur les risques de sécurité et les vulnérabilités majeures identifiées.

-Soumission des mesures correctives associées.

Support pour le management :

-Résumé rappelant le contexte et les objectifs.

-Description du déroulement du test d'intrusion.

-Présentation des résultats sous forme d'indicateurs chiffrés ou graphiques.

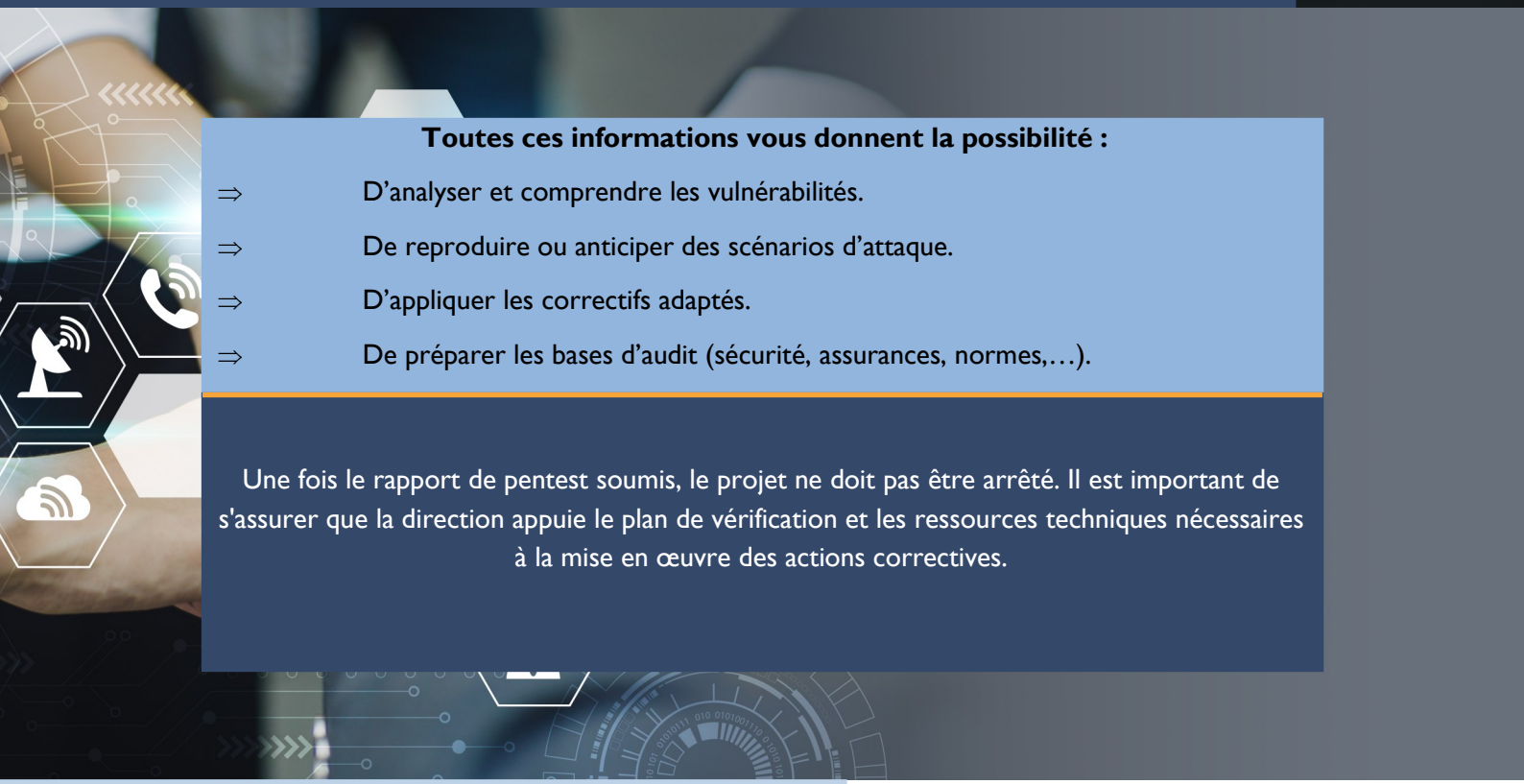
-Soumission d'un calendrier pour les corrections à mettre en œuvre.

Support technique :

-Synthèse du rapport de management.

-Rapport détaillé des failles techniques relevées et moyens techniques utilisés.

-Présentation des points techniques des différentes failles sécuritaires.



Toutes ces informations vous donnent la possibilité :

⇒ D'analyser et comprendre les vulnérabilités.

⇒ De reproduire ou anticiper des scénarios d'attaque.

⇒ D'appliquer les correctifs adaptés.

⇒ De préparer les bases d'audit (sécurité, assurances, normes,…).

Une fois le rapport de pentest soumis, le projet ne doit pas être arrêté. Il est important de s'assurer que la direction appuie le plan de vérification et les ressources techniques nécessaires à la mise en œuvre des actions correctives.

myDigitplace
9 chemin de la Salvetat 31770 Colomiers
05.61.15.62.16
commercial@mydigitplace.com