Tests et audit de sécurité

Contact: Jean-Jacques Fulgoni
✉ jeanjacques.fulgoni@perenne-it.fr
✆ 01 39 23 97 68

Le contexte

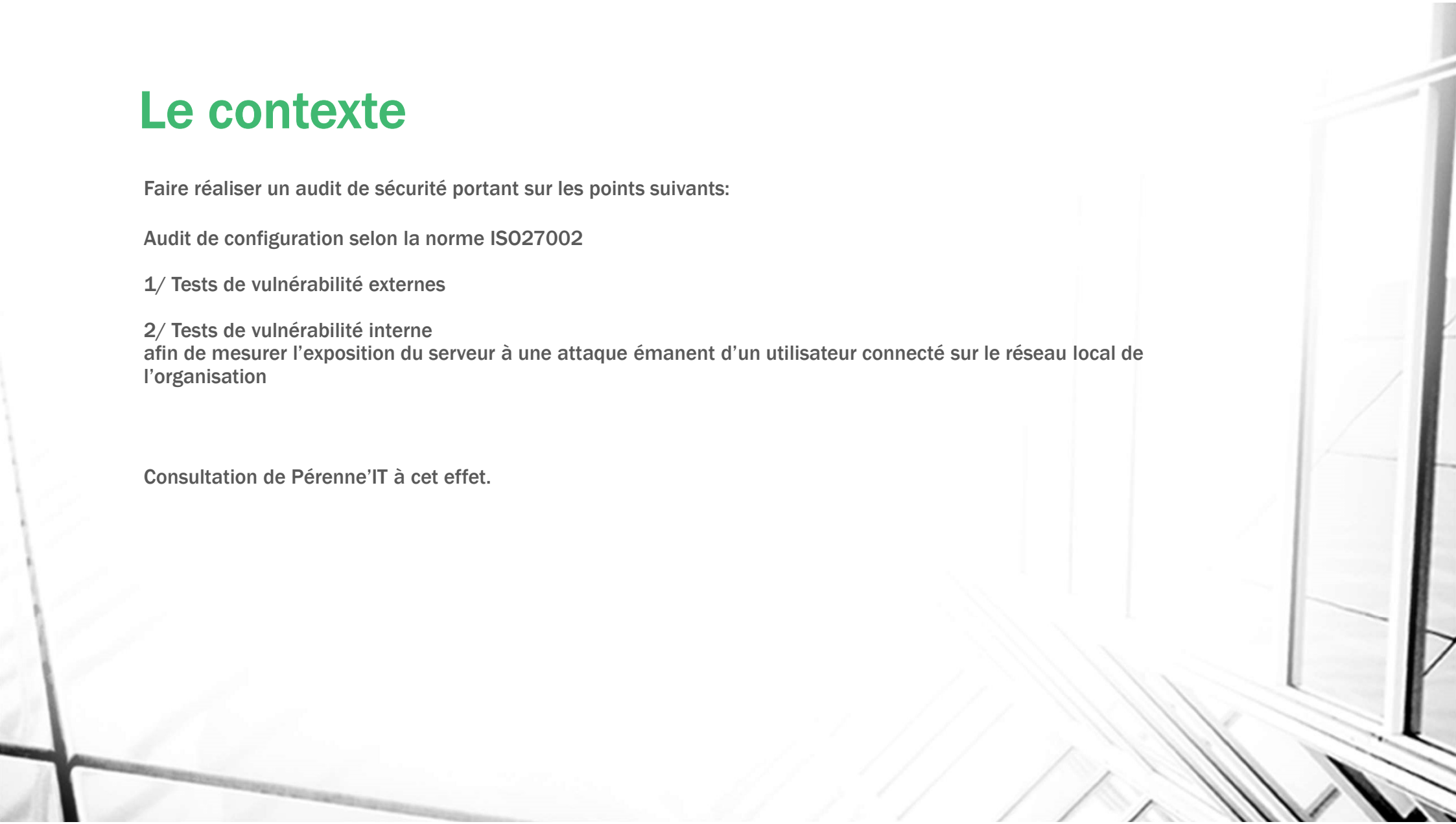
Faire réaliser un audit de sécurité portant sur les points suivants:

Audit de configuration selon la norme ISO27002

1/ Tests de vulnérabilité externes

2/ Tests de vulnérabilité interne
afin de mesurer l'exposition du serveur à une attaque émanent d'un utilisateur connecté sur le réseau local de l'organisation

Consultation de Pérenne'IT à cet effet.



Phase 1 Démarche proposée

Phase de découverte

Cette phase encore appelée phase de repérage consiste à analyser à partir d'une plage d'adresses publiques fournie par le client l'environnement d'un site, d'identifier les éléments visibles dans le périmètre, en vue de préparer la batterie de tests appropriée pour identifier les vulnérabilités

Phase d'identification

A l'aide d'outils spécialisés (notamment des scanners), d'investigations, ingénierie sociale, etc..; examen et validation des vulnérabilités. En fonction des résultats obtenus lors de ces deux phases, des tests complémentaires peuvent être menés de manière à éliminer un maximum de faux positifs.

Thèmes étudiés

Les vulnérabilités sont étudiées et recherchées à 2 niveaux :

- · Au niveau réseau & système: (notamment ports actifs, versions software,…)
- · Au niveau applicatif (exemple : Injection SQL, Cross Site Scripting XSS, débordement de mémoire, prévention GHDB,…)

Exploitation et rapport

Exploitation des informations recueillies :

· Analyse des résultats

· Rédaction du compte rendu

Livrables

- Un document de synthèse en français décrivant les diligences menées, les principales vulnérabilités et recommandations associées
- Des annexes techniques en anglais détaillant le détail des scans effectués

Phase 2 Audit de configuration

Sur la base d'un périmètre défini au préalable et en fonction des résultats des tests de vulnérabilité, nous proposons un audit de configuration s'appuyant sur le référentiel de sécurité ISO 27000

Audit de configuration

L'audit de configuration a pour objectif de vérifier le paramétrage de vos équipements par rapport aux risques de sécurité. Le résultat de l'audit permet de déterminer si l'implémentation technique auditée est conforme aux bonnes pratiques de sécurité et ne présente pas de risque pour le reste du système d'information

Méthodologie

L'audit s'appuiera sur le référentiel ISO 27002 , il comprend des études de configurations techniques, de documentations, entretiens avec les équipes de la DSI et prestataires externes éventuellement concernés

Exploitation et rapport

Exploitation des informations recueillies :

· Analyse des résultats

· Rédaction du compte rendu

Livrables

- Un document de synthèse en français décrivant les diligences menées, les principales vulnérabilités et recommandations

Associées qui pourront servir de base à l'élaboration d'un plan d'action

- Un synthèse ISO 27000 sur le périmètre étudié
- Des annexes techniques en anglais détaillant le détail des scans effectués

Charge de travail

Dépend si test externe et interne et du nombre d'adresse IP à Tester

Pré-requis aux tests de vulnérabilité

Avertissement

Malgré une expérience et une méthodologie éprouvée, les tests de vulnérabilité peuvent perturber le fonctionnement des systèmes ou des applications:

Consommation de bande passante : Rarement problématique, les tests de vulnérabilité consomment peu de bande passante. Toutefois, si cela devait être un souci, merci de nous préciser vos contraintes : les dates, les horaires à éviter…

Disponibilité des équipements : (rare) lorsque les équipements sont confrontés à des activités inhabituelles, leurs comportements peuvent être chaotiques. Il est conseillé que les personnes responsables de ces équipements possèdent nos coordonnées afin de nous joindre en cas de problèmes.

Disponibilité des logiciels : Des applications vulnérables peuvent « crasher » suite à des tests basiques. Même si les auditeurs prennent toutes leurs précautions, le risque est toujours existant. Il est conseillé de posséder des sauvegardes des systèmes et des bases de données

Conditions de réalisation des tests de vulnérabilité

Pré requis côté Client :

Pour le bon déroulement des tests de vulnérabilité, vous devrez nous fournir :

- Un contact à appeler en cas de besoin durant l'audit (numéro de téléphone, adresse mail), et un administrateur disponible
- Une liste complète des systèmes à auditer (adresses IP, noms d'hôte)
- Une autorisation légale pour effectuer les tests signé par un représentant légal du client. Cette autorisation précise le périmètre et la période des tests.
- Une notification spéciale sera nécessaire si l'un des systèmes ciblés est hébergé ou appartenant à un tiers.

· Lors de notre intervention, le système à évaluer doit être en état de fonctionnement, et actif

· Par mesure de précaution, toutes les sauvegardes nécessaires doivent avoir été faites préalablement aux tests

· Lorsqu'un site Web propose à une population déterminée (clients/fournisseurs/partenaires) un accès restreint sécurisé par login/password, un code d'accès doit nous être communiqué afin de tester les risques associés à cette population.

PÉRENNE'IT

· PÉRENNE'IT s'engage par accord de confidentialité à ne divulguer aucune information confidentielle de l'environnement du Client

· PÉRENNE'IT s'engage à limiter les tests techniques à des tests non destructifs. En aucun cas, ils ne peuvent donc porter atteinte à la disponibilité ou à la sécurité du système d'information.

· Les tests de vulnérabilités sont effectués pendant une période limitée dans le temps et définie au préalable avec le Client