Test d'intrusion et Cybermenaces

détectez vos failles avant qu'un hacker ne le fasse

pérenne IT

Qu'est-ce qu'un test d'intrusion ?

Un test d'intrusion, également connu sous le nom de "pentest" (pour "penetration test"), est une évaluation proactive de la sécurité d'un système informatique, d'un réseau ou d'une application. Il permet d'évaluer le niveau de sécurité d'un périmètre en utilisant les mêmes outils et méthodes qu'un véritable attaquant.
Lors d'un pentest, différents scénarios peuvent être proposés.

Chez OWN, nous proposons deux types de scénarios :

- Le test d'intrusion dit « boite noire » : Le pentester simule un attaquant disposant seulement des adresses IP / URL du périmètre. (ex: contournement d'authentification, vol de données, …) –
  Ce scénario est catégorisé comme non authentifié
- Le test d'intrusion dit « boite grise » : Des accès représentatifs des usages réels seront transmis à l'auditeur afin de simuler un utilisateur malveillant ou compromis (ex: défaut de cloisonnement, élévation de privilège, vol de données, …) – Ce scénario est catégorisé comme un scénario authentifié

Ces tests seront effectués selon la méthodologie OWASP ou OSSTMM et les éventuels risques seront mesurés en suivant la matrice de calcul de l'ANSSI, garantissant une exhaustivité des tests et une évaluation compréhensible du niveau de sécurité de la plateforme auditée.
Périmètre : Application web, Application mobile, Réseau interne (AD), Client lourd, objet connecté, équipement physique …
Les tests de type déni de service et d'ingénierie sociale (phishing) sont hors périmètre dans le cadre de ce genre de prestation

Dans quels cas doit-on réaliser des tests d’intrusion ?

Dans plusieurs situations clés, il est important de réaliser des tests d’intrusion pour assurer la sécurité et l'intégrité des systèmes informatiques, des réseaux et des applications, un test d'intrusion est fortement recommandé :

- **Lancement d'un nouveau système ou application :**

Avant de déployer un nouveau système, une nouvelle application ou une mise à jour majeure, il est nécessaire de réaliser un test d'intrusion pour identifier et corriger les vulnérabilités potentielles. Cela permet de s'assurer que les nouvelles fonctionnalités ou modifications n'introduisent pas de failles de sécurité qui pourraient être exploitées par des attaquants. Par exemple, un test d'intrusion peut révéler des problèmes de configuration, des bugs logiciels ou des faiblesses dans les mécanismes d'authentification.

- **Changements significatifs dans l'infrastructure :**

Votre organisation effectue des modifications importantes à son SI comme l’ajout de nouveaux serveurs ou l'intégration de nouvelles technologies (par exemple, le passage à des solutions cloud ou l'adoption de l'IoT) ? Alors un test d'intrusion vous aidera à vous s'assurer que ces changements n'introduisent pas de nouvelles failles de sécurité. Les tests permettent de vérifier que les nouvelles composantes sont correctement sécurisées et intégrées dans l'environnement existant.

- **Conformité réglementaire :**

De nombreuses réglementations et normes de sécurité (comme PCI-DSS pour les paiements par carte, HIPAA pour les données de santé, ou GDPR pour la protection des données personnelles) exigent des tests d'intrusion réguliers pour assurer la conformité. Il est donc important de planifier ces tests en fonction des exigences légales et réglementaires applicables à votre secteur. Par exemple, PCI-DSS nécessite des tests d'intrusion annuels et après tout changement significatif dans l'environnement de paiement.

Dans quels cas doit-on réaliser des tests d’intrusion ?

- **Évaluation périodique :**

Même en l'absence de changements majeurs ou d'incidents, il est recommandé de réaliser des tests d'intrusion de manière périodique pour s'assurer que les systèmes restent sécurisés face à l'évolution constante des menaces. Les cybermenaces évoluent rapidement, et ce qui était sécurisé il y a un an peut ne plus l'être aujourd'hui. Une évaluation régulière permet de rester proactif et de détecter les nouvelles vulnérabilités avant qu'elles ne soient exploitées.

- **Acquisition ou fusion d'entreprises :**

Lors de l'acquisition d'une nouvelle entreprise ou de la fusion avec une autre organisation, il est important de réaliser des tests d'intrusion pour évaluer la sécurité des systèmes et des réseaux intégrés. Cela permet de s'assurer que les infrastructures fusionnées ne présentent pas de failles de sécurité qui pourraient compromettre l'ensemble de l'organisation. Par exemple, un test d'intrusion peut révéler des vulnérabilités dans les systèmes de l'entreprise acquise qui doivent être corrigées avant l'intégration complète.

- **Déploiement de nouvelles fonctionnalités :**

Si vous ajoutez de nouvelles fonctionnalités à une application existante, un test d'intrusion peut aider à s'assurer que ces ajouts n'introduisent pas de nouvelles vulnérabilités. Par exemple, l'ajout d'une nouvelle API ou d'une fonctionnalité de paiement en ligne peut créer des points d'entrée potentiels pour les attaquants. Un test d'intrusion permet de vérifier que ces nouvelles fonctionnalités sont sécurisées et ne compromettent pas l'ensemble de l'application.

En résumé, les tests d'intrusion doivent être réalisés régulièrement et dans des situations spécifiques pour garantir que les systèmes, les réseaux et les applications restent sécurisés contre les menaces potentielles.

Pourquoi faire un test d’intrusion ?

Voici quelques-unes des principales utilités d'un test d'intrusion :

- **Identification des vulnérabilités :**

Les tests d'intrusion permettent de détecter les failles de sécurité avant qu'elles ne soient exploitées par des attaquants malveillants. Cela inclut la découverte de bugs logiciels, de configurations incorrectes, de mots de passe faibles, et de toute autre faille qui pourrait être utilisée pour compromettre le système. En identifiant ces vulnérabilités, les organisations peuvent prendre des mesures correctives avant qu'une attaque réelle ne se produise.

- **Évaluation des risques :**

Ils aident à comprendre les risques potentiels et l'impact d'une attaque réussie sur les systèmes et les données de l'organisation. Par exemple, un test d'intrusion peut révéler qu'une vulnérabilité dans une application web pourrait permettre à un attaquant d'accéder à des informations sensibles, de perturber les opérations ou de causer des pertes financières. Cette évaluation permet aux organisations de prioriser les actions de remédiation en fonction de la criticité des risques identifiés.

- **Conformité réglementaire :**

De nombreuses réglementations et normes de sécurité (comme PCI-DSS pour les paiements par carte, HIPAA pour les données de santé, ou GDPR pour la protection des données personnelles) exigent des tests d'intrusion pour assurer la conformité. En réalisant ces tests, les organisations peuvent démontrer qu'elles prennent des mesures proactives pour protéger les données sensibles et se conformer aux exigences légales et réglementaires.

Pourquoi faire un test d’intrusion ?

- **Amélioration des mesures de sécurité :**

Les résultats des tests d'intrusion fournissent des recommandations pour renforcer les défenses et améliorer les politiques de sécurité. Par exemple, ils peuvent suggérer de mettre à jour des logiciels, de renforcer les configurations de sécurité, d'implémenter des solutions de détection et de réponse aux incidents, ou de former le personnel aux meilleures pratiques de sécurité. En suivant ces recommandations, les organisations peuvent améliorer leur posture de sécurité globale et réduire les risques d'attaques futures.

Un test d'intrusion, est une évaluation de la sécurité de vos systèmes, réseaux et applications, simulant les actions d'un attaquant. Il est particulièrement important lors du déploiement d’une nouvelle application, l’intégration d’une évaluation majeure ou lors d’une acquisition ou fusions d'entreprises pour sécuriser les infrastructures intégrées. Une évaluation régulière est recommandée pour faire face à l'évolution constante des cybermenaces. Ces tests permettent de rester proactif et de détecter les vulnérabilités avant qu'elles ne soient exploitées par de réels attaquants.

🔐 Pentest terminé. Et maintenant ?

La checklist claire pour passer à l'action, sans paniquer.

Un test d'intrusion, ce n'est pas un verdict.
C'est une photographie de vos vulnérabilités à un instant T.
Et surtout, c'est le point de départ d'un plan d'amélioration.

Voici une checklist opérationnelle pour transformer le rapport en actions concrètes.
À adapter selon vos moyens, vos priorités et vos réalités.

✅ Étape 1 — Comprendre avant d'agir

📖 *Lire. Comprendre. Expliquer.*

- Avez-vous lu tout le rapport, pas seulement les grandes lignes ?
- Avez-vous compris chaque type de faille (technique, logique, humaine) ?
- Les résultats ont-ils été partagés aux bons interlocuteurs internes (DSI, RSSI, métiers) ?
- Les risques métiers ont-ils été croisés avec les failles techniques ?

Pentest terminé. Et maintenant ?

Étape 2 — Hiérarchiser les risques

Classer pour mieux décider.

- Avez-vous trié les failles : critique / élevée / modérée / faible ?
- Un plan d'action a-t-il été défini avec des priorités réalistes ?
- Des validations spécifiques sont-elles nécessaires (métier, juridique, partenaires) ?
- Avez-vous repéré les "quick wins" à corriger rapidement ?

Étape 3 — Corriger avec méthode

Appliquer les patchs, revoir les configs.

- Les mises à jour critiques ont-elles été déployées ?
- Les configurations sensibles ont-elles été revues (mots de passe, droits, exposition) ?
- Les applications ou systèmes concernés ont-ils été corrigés ?
- Avez-vous testé que tout fonctionne après correction (test de non-régression) ?

Étape 4 — Renforcer la sécurité

Aller plus loin que la simple correction.

- Avez-vous ajouté des mesures complémentaires (WAF, segmentation, durcissement) ?
- Les droits utilisateurs ont-ils été revus selon le principe du moindre privilège ?
- Une sensibilisation sécurité a-t-elle été organisée ?
- Les procédures internes ont-elles été adaptées aux leçons du pentest ?

Pentest terminé. Et maintenant ?

Étape 5 — Suivre et progresser

Mesurer, recontrôler, apprendre.

- Un suivi clair est-il en place pour les actions en cours ?
- Un re-pentest est-il prévu (même partiel ou ciblé) ?
- Un retour d’expérience a-t-il été partagé ?
- L’équipe IT se sent-elle soutenue et non jugée dans cette phase ?

Petit à petit, la sécurité se construit

On ne corrige pas tout en un jour, et ce n’est pas grave.
L’important, c’est de savoir où vous en êtes, où vous allez, et avec qui.

Chez Pérenne'IT, on ne vous lâche pas avec un rapport et des bonnes intentions.
On vous aide à prioriser, corriger, renforcer, et à avancer à votre rythme — sans magique.

Qui sommes-nous ?

Pérenne'IT, initialement un cabinet de conseil spécialisé en sécurité, a évolué depuis une dizaine d'années pour mieux répondre aux besoins des PME en tirant parti du Cloud Computing.

Fidèle à son expertise en cybersécurité, l'entreprise se distingue en intervenant à toutes les étapes du cycle de vie du système d'information, depuis les audits jusqu'à l'exploitation sécurisée, en passant par la remédiation, la modernisation et la migration des systèmes.

Elle propose également de la sensibilisation et de l'accompagnement pour les équipes.

Partenaire expert de Microsoft 365, Microsoft Azure et OVHcloud.

info@perenne-it.fr
WWW.perenne-it.fr