

# Le pentest

# Table des matières

<b>I. Qu'est-ce qu'un pentest ?</b>	<b>3</b>
<b>II. Exercice : Quiz</b>	<b>5</b>
<b>III. Pourquoi faire un audit de configuration ?</b>	<b>5</b>
<b>IV. Exercice : Quiz</b>	<b>7</b>
<b>V. Se poser les bonnes questions pour appréhender les risques</b>	<b>8</b>
<b>VI. Exercice : Quiz</b>	<b>9</b>
<b>VII. Essentiel</b>	<b>10</b>
<b>VIII. Auto-évaluation</b>	<b>10</b>
<b>Solutions des exercices</b>	<b>11</b>

## I. Qu'est-ce qu'un pentest ?

**Durée :** 1 h30

**Environnement de travail :** un PC / Une Tablette / Un smartphone

**Pré-requis :** aucun

### Contexte

Pour protéger son entreprise, il faut être conscient de l'état de sécurité du matériel informatique. Pour vérifier cet état, il est possible de réaliser un test d'intrusion ou pentest. Une fois ce test réalisé, il sera possible pour l'entreprise d'analyser la situation actuelle et de prendre des décisions pour la protéger.

Mais avant un pentest, il y a la réalisation d'un audit de configuration permettant d'identifier les risques de sécurité de votre configuration système. Cela vous permettra de garder votre entreprise à l'abri des piratages. En effet, la plupart d'entre eux pourraient être évités facilement. Vous aurez ainsi une meilleure visibilité sur la configuration de votre système.

Les entreprises doivent être capables d'évaluer les risques liés à l'accès des ressources. Pour cela, elles peuvent mettre en place des stratégies d'évaluation et doivent se poser les bonnes questions concernant l'accès à ces ressources.

### Définition

Pour améliorer la sécurité de l'entreprise, il est important de mettre en place différents audits permettant de comprendre l'état dans lequel se trouve le matériel. Les différents audits qui peuvent être mis en place sont les suivants :

- Audit organisationnel
- Audit d'intrusion
- Audit technique
- Test d'intrusion

Dans ce chapitre, nous allons nous intéresser aux différents tests d'intrusion ou pentest qui existent et quelle est l'utilité de ces tests.

Un test d'intrusion aussi appelé pentest (test de pénétration) est une méthode permettant l'évaluation de la sécurité d'un système informatique ou d'un réseau. Ce test est effectué par un pentesteur.

Le test d'intrusion est donc différent de l'audit de sécurité. En effet l'audit de sécurité permet l'évaluation de la sécurité du système et des applications en suivant un référentiel constitué de politique de sécurité informatique de l'entreprise, de textes de loi, de bonnes pratiques, de normes, et de références. Le test d'intrusion a pour but d'évaluer la sécurité par rapport aux différentes pratiques employées par les pirates informatiques.

Le test d'intrusion n'est pas non plus à confondre avec le scanner de vulnérabilité. Un scanner de vulnérabilité est une démarche qui consiste à utiliser des outils automatisés afin d'analyser quels sont les ports ouverts sur une machine donnée présente sur le réseau de l'entreprise. Il ne couvre donc qu'une partie restreinte des vulnérabilités et la démarche d'automatisation utilisée limite les possibilités de découverte de failles.

Un test d'intrusion permet d'identifier le niveau de sécurité présent dans le Système d'Information de l'entreprise. Il s'agit d'une attaque contrôlée qui révélera le niveau de sécurité actuel. Le testeur pourra ainsi identifier les points de vulnérabilité du système ainsi que déterminer quels sont les correctifs à mettre en place. Des données précises seront récupérées sur le type d'intrusion qui pourrait être réalisé par un hacker en traversant les mécanismes de sécurité informatique.

Il existe différents tests d'intrusion pouvant porter sur différents aspects de la sécurité du système d'information.

### Attention

Attention ! Un test d'intrusion est différent d'un test de vulnérabilité. Il ne faut donc pas les confondre. En effet, ces 2 tests n'ont pas les mêmes objectifs. Ainsi, un test de vulnérabilité sera limité à identifier des failles courantes et utiliser des outils automatiques. Un test d'intrusion aura pour objectif d'intégrer des recherches de failles logiques qui seraient indétectables par des outils automatiques. En plus de cela, il devra intégrer des étapes d'exploitation manuelles des failles découvertes. En conclusion, un test d'intrusion est plus complet et permet de déterminer quel est l'impact réel et quels sont les différents types de vulnérabilité.

## Les différents tests d'intrusion

**Le test en boîte noire :** le test en boîte noire consiste à la réalisation d'un test d'intrusion en exploitant la moindre information du réseau. Ce test est réalisé dans des conditions imitant une attaque par un pirate informatique venant de l'extérieur.

**Le test en boîte blanche :** l'objectif de ce test est d'avoir accès à la totalité des informations sur le système pour le testeur. Il s'agit ici d'une autre vision d'une personne qui serait en possession des mots de passe permettant d'avoir un accès administrateur. Cette approche est celle qui permet de détecter le plus de failles de sécurité.

**Le test en boîte grise :** ce test consiste à essayer de s'introduire dans un système d'information en disposant seulement de peu d'informations concernant l'organisation du système. Il s'agit donc d'un test simulant une attaque par un client, un prestataire, ou un salarié malhonnête.

## La réalisation du test d'intrusion

Un test d'intrusion doit suivre un schéma comportant au minimum 4 étapes. A l'issue de ces 4 étapes, le test d'intrusion sera considéré comme terminé.

Pour réaliser un test d'intrusion il faut d'abord commencer par définir le périmètre de test. Ce périmètre peut être défini après avoir réalisé un audit de sécurité informatique. L'analyse de risques obtenus à l'aide de cet audit permet d'identifier les informations sensibles à protéger et les objectifs de sécurité.

La deuxième étape d'un test d'intrusion est le choix de la stratégie ainsi que le type de test d'intrusion privilégié. Cette stratégie sera mise en place en fonction du niveau d'information connu et mis à disposition. Il faudra également déterminer le niveau d'accès utilisateur ainsi que le niveau d'accès au réseau. C'est à ce moment-là qu'on parlera de boîte blanche, boîte noire ou boîte grise. Les conditions de cette stratégie dépendent du type de piratage que vous souhaitez reproduire.

La troisième étape est la plus importante, Elle consiste à lancer une attaque en fonction du scénario d'attaque choisi. Le testeur devra effectuer différents essais en fonction du périmètre déterminé ainsi que de la stratégie choisie.

La quatrième et dernière étape du processus de test d'intrusion est la création d'un rapport. Le rapport devra révéler les informations suivantes :

- Une liste des vulnérabilités ayant été découvertes,
- Le niveau de risque lié aux vulnérabilités,
- La probabilité d'occurrences,
- L'impact que peut avoir la défaillance sur le système,
- Une liste des recommandations qui permettront de pallier ces vulnérabilités et ainsi diminuer les risques dans l'entreprise.

Les étapes du test d'intrusion peuvent néanmoins changer en fonction des stratégies adoptées lors de la procédure. En effet, celui-ci peut-être interne ou externe.

- Le test d'intrusion interne permet au testeur d'être directement placé sur le réseau cible.
- Le test d'intrusion externe permet de placer le testeur à l'extérieur du réseau cible.

Une fois le test d'intrusion réalisé, les administrateurs systèmes et réseaux pourront mettre en place une stratégie leur permettant de sécuriser le réseau en le protégeant face aux attaques éventuelles de personnes mal intentionnées. Le test d'intrusion apparaît donc comme un élément clé de la cybersécurité d'une entreprise.

## Exercice : Quiz

[solution n°1 p.13]

### Question 1

Un test d'intrusion doit suivre un schéma comportant au minimum 3 étapes.

- ☐ Vrai
- ☐ Faux

### Question 2

La deuxième étape d'un test d'intrusion est la plus importante, il s'agit du choix de la stratégie.

- ☐ Vrai
- ☐ Faux

### Question 3

À la fin du processus, il est primordial de rédiger un rapport.

- ☐ Vrai
- ☐ Faux

### Question 4

Le test d'intrusion interne permet de placer le testeur à l'extérieur du réseau cible.

- ☐ Vrai
- ☐ Faux

### Question 5

Pour améliorer la sécurité de l'entreprise, il est important de mettre en place directement un test d'intrusion.

- ☐ Vrai
- ☐ Faux

## III. Pourquoi faire un audit de configuration ?

L'audit de configuration fait partie des éléments à réunir avant un pentest. En effectuant un audit de configuration, vous réalisez une évaluation technique de la configuration des composants du système d'information. En faisant cela, vous vous assurez que les mesures de sécurité respectent bien les bonnes pratiques en matière de sécurité. Pour effectuer un audit de configuration, vous devez vérifier les équipements réseaux, les systèmes d'exploitation, les logiciels, les applications, les bases de données, etc. L'intérêt de cet audit est d'éviter que les attaquants ne s'en prennent aux défauts de configuration du réseau informatique. Le faire avant votre pentest vous permettra de vérifier la solidité de votre architecture.

### Définition

Un audit de configuration permet de détecter les modifications et d'évaluer la configuration du réseau afin de limiter les risques.

Comme toutes les démarches d'audit, l'audit de configuration s'appuie sur le référentiel de l'ANSSI.

Un audit de configuration permet de :

- Évaluer le niveau de sécurité des machines.
- Comparer la configuration présente sur les différents appareils et les nouvelles technologies qui amélioreraient la sécurité.
- Définir le plan d'action technique à privilégier.
- Vérifier que les bonnes pratiques sont mises en place sur tout le système.

Pour réaliser un audit de sécurité sur un pare-feu, Il faudra vérifier la configuration de celui-ci, l'auditeur devra avoir récupéré au préalable la configuration du pare-feu.

L'objectif de l'audit de configuration :

- Il vous permettra de découvrir les inexactitudes de configuration présentes sur les différentes machines du système.
- Il permet d'identifier les problèmes dû à l'obsolescence de certains logiciels comme les firmwares.
- Il permet une révision complète des fichiers de configuration et des règles présents sur les différentes machines du réseau comme les routeurs, les firewalls, les switch, etc.

Une fois l'audit réalisé, le système sera mieux préparé aux attaques.

### La réalisation d'un audit de configuration

Un audit de configuration représente bien plus qu'une simple formalité. Il permet de mettre en évidence les erreurs de sécurité présente et représente donc un fondement essentiel de la cybersécurité.

Pour que l'audit de sécurité soit mené à bien, il faut que les éléments de configuration des machines cibles auditées soient fournis à l'auditeur. Ces configurations peuvent-être récupérée manuellement ou automatiquement à partir d'accès privilégiée aux machines cibles audités. Ils peuvent être utilisés sous la forme de fichiers de configuration ou de capture d'écran.

Avant de réaliser l'audit, l'auditeur doit avoir récupéré tous les accords nécessaires à la manipulation des données présentes sur les différentes machines du réseau.

L'auditeur devra, conformément à l'état de l'art, vérifier la sécurité des configurations des équipements suivants :

- Les équipements de type routeur, switch, borne wifi, etc. (Équipement réseau filaire ou sans fil).
- Les équipements de sécurité tels que les pare-feu, les proxys ils devront vérifier les règles de filtrage, les chiffreurs, etc.).
- Les systèmes d'exploitation.
- Les systèmes de gestion de bases de données.
- Les services d'infrastructure.
- Les serveurs d'applications.
- Les postes de travail.
- Les téléphones, tablettes, etc.
- Les environnements de virtualisation.

Une fois l'audit réalisé, des recommandations devront être émises par l'auditeur. Elles doivent concerner les éléments suivants :

- Le système d'authentification (est-il puissant ou faible ?).
- Un mécanisme de cryptographie est-il bien mis en place sur le réseau ? Est-il efficace ?
- Quelles sont les règles de filtrage utilisées ? (Entrée, sortie, routage, NAT, etc.).
- Les différents réseaux sont-ils bien segmentés ? (VLAN, etc.).
- Les bonnes pratiques sont-elles bien appliquées au systèmes d'exploitation, des configurations des serveurs applicatifs et des services d'infrastructure ?

L'audit de configuration n'est qu'une petite partie de la méthode d'Audit proposé par l'ANSSI. Ainsi, un Audit de configuration doit être complété de différents audits importants pour la mise en sécurité de votre réseau (audit applicatif, de code source, de centre de serveur, d'architecture réseau, organisationnel, etc.).

L'audit de configuration peut servir de base à la réalisation d'un test d'intrusion et représente un réel socle à la réalisation de différents tests. Une faille découverte lors d'un audit de configuration pourrait mener à son exploitation lors d'un test d'intrusion.

## Exercice : Quiz

[solution n°2 p.13]

### Question 1

Un audit de configuration permet de mettre en évidence les erreurs de sécurité présentes.

- ☐ Vrai
- ☐ Faux

### Question 2

Il n'y a pas de pré-requis avant de démarrer l'audit.

- ☐ Vrai
- ☐ Faux

### Question 3

En effectuant un audit de configuration, vous réalisez :

- ☐ Un test de la configuration des composants du système d'information
- ☐ Une évaluation technique de la configuration des composants du système d'information

### Question 4

Vous devez vérifier uniquement les équipements réseaux, les systèmes d'exploitation.

- ☐ Vrai
- ☐ Faux

### Question 5

Un audit de configuration permet de définir le plan d'action technique à privilégier.

- ☐ Vrai
- ☐ Faux

## V. Se poser les bonnes questions pour appréhender les risques

Il existe plusieurs questions qu'un RSSI doit se poser afin de sécuriser l'accès aux différentes ressources. Voici une liste non exhaustive des différentes questions à se poser (selon l'ANSSI) permettant la sécurisation des ressources.

### Définition ANSSI

Selon le site officiel de l'ANSSI<sup>1</sup>, cette dernière est un « *Service du Premier ministre, rattaché au Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)* ». L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cybersécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des Opérateurs d'Importance Vitale (OIV). « *Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.* »

### Les questions à se poser

#### Combien de personnes disposent de droits administrateur, qui sont ces personnes ?

Seules les personnes dont l'accès est nécessaire et indispensable pour la réalisation de leur mission doivent détenir des privilèges élevés. Toutes les personnes disposant de ces droits doivent être énumérées et nommées dans une liste qui doit rester à jour. En effet, les comptes privilégiés ont des accès stratégiques aux machines, ils représentent donc un risque accru d'attaque.

#### Les mots de passe sont-ils uniques ?

Ne mettez pas de mots de passe en commun. Chaque utilisateur doit avoir un mot de passe respectant les consignes de sécurité (long, caractères spéciaux, chiffres) et celui-ci doit rester personnel.

#### Les administrateurs disposent-ils de mots de passe différents ?

Afin de rendre les actions traçables, tous les administrateurs doivent disposer d'un compte individuel avec des mots de passe différents.

#### Les administrateurs ont-ils plusieurs comptes avec différents droits ?

Les comptes avec des droits d'administration élevés doivent être réservés aux tâches administratives nécessitant obligatoirement ces droits. Pour les actions ne nécessitant pas d'accès administrateur comme lire ses mails ou naviguer sur internet, des comptes avec moins de droits suffisent.

#### Avez-vous vérifié qui a accès aux messageries des directeurs et PDG ?

Pensez à surveiller régulièrement les accès aux boîtes de messagerie des dirigeants.

#### Pensez-vous à regarder les logs régulièrement ?

En analysant les journaux, vous pourrez vérifier tous les événements se déroulant, notamment aux heures critiques comme la nuit ou le week-end.

#### Pensez-vous à tenir à jour l'ensemble du système ?

Pour éviter tout piratage lié à des vulnérabilités du système d'exploitation, pensez à mettre à jour régulièrement tout le système à l'aide d'un outil de centralisation et de gestion des mises à jour. Pensez également à mettre à jour les logiciels.

#### Utilisez-vous toujours des systèmes d'exploitation obsolètes ?

Si vous utilisez encore de vieilles versions de Windows comme Windows XP et que la migration vers une version plus récente n'est pas possible, pensez à isoler la machine du réseau. Ainsi, elle ne pourrait pas infecter le réseau en cas de piratage.

<sup>1</sup> <https://www.ssi.gouv.fr/agence/missions/lanssi-en-un-coup-doeil/>



**Avez-vous mis en place une cartographie du réseau ?**

Pensez à mettre en place une cartographie précise de tous les éléments du réseau. Elle vous permettra de réagir rapidement en cas d'incident.

**Avez-vous répertorié tous les accès internet ?**

Bien connaître tous les accès réseau de l'entreprise est primordial pour surveiller toutes les entrées et les sorties de flux.

**Pensez-vous à supprimer les comptes après le départ d'un employé ?**

Après le départ d'un employé, il faut supprimer son compte immédiatement. Si ce n'est pas le cas, un attaquant pourrait utiliser ce compte. Pensez donc à mettre en place une procédure et à mettre des dates d'expiration pour les stagiaires et prestataires.

**Avez-vous désactivé l'exécution automatique des clés USB ?**

Les clés USB représentent un réel danger pour les ressources de l'entreprise. Si leur exécution automatique n'est pas supprimée, alors un virus pourrait entrer sur le système dès l'insertion d'une clé. Vous pourriez également bloquer les clés USB inconnues.

**Laissez-vous les utilisateurs installer des applications ?**

Restreindre l'installation d'applications pour les utilisateurs permet de limiter les risques concernant les environnements tels que Java, Adobe Air ou Perl. En effet, ceux-ci permettent l'exécution de logiciels sans contraintes de stratégies de restriction d'exécution logicielle.

**Avez-vous prévu un plan en cas d'intrusion majeure du système ?**

En cas de crise (intrusion d'ampleur) toutes les heures passées peuvent empirer la situation. Vous devez donc au préalable avoir prévu un plan (tant au niveau organisationnel que technique) qui vous permettra de répondre à la situation de crise au plus vite.

**Que faites-vous lorsqu'un poste de travail a été infecté ?**

En infectant un PC, un attaquant se crée des portes d'entrée dans tout le réseau. Il ne suffit donc pas de supprimer le virus de l'ordinateur infecté, mais de vérifier tout le réseau.

**Exercice : Quiz**

[solution n°3 p.14]

## Question 1

L'ANSSI est un organisme privé.

- ☐ Vrai
- ☐ Faux

## Question 2

Les employés du service informatique n'ont besoin que d'un compte administrateur.

- ☐ Vrai
- ☐ Faux

## Question 3

Les utilisateurs ne doivent pas avoir de mots de passe en commun.

- ☐ Vrai
- ☐ Faux

## Question 4

Pourquoi les administrateurs doivent-ils utiliser des comptes individuels et personnels pour se connecter aux différentes machines du réseau ?

- ☐ Pour être organisés
- ☐ Pour avoir une traçabilité

#### Question 5

Pour vérifier tous les éléments s'étant passés sur le réseau, je dois regarder dans les logs.

- ☐ Vrai
- ☐ Faux

## VII. Essentiel

Un test d'intrusion, aussi appelé pentest (test de pénétration) est une méthode permettant l'évaluation de la sécurité d'un système informatique ou d'un réseau. Ce test est effectué par un pentesteur. Le test d'intrusion est donc différent de l'audit de sécurité. En effet l'audit de sécurité permet l'évaluation de la sécurité du système et des applications en suivant un référentiel constitué de politique de sécurité informatique de l'entreprise, de textes de loi, de bonnes pratiques, de normes, et de références.

Le test d'intrusion a pour but d'évaluer la sécurité par rapport aux différentes pratiques employées par les pirates informatiques. Un test d'intrusion permet d'identifier le niveau de sécurité présent dans le Système d'Information de l'entreprise. Il s'agit d'une attaque contrôlée qui révélera le niveau de sécurité actuel. Le testeur pourra ainsi identifier les points de vulnérabilité du système ainsi que déterminer quels sont les correctifs à mettre en place. Des données précises seront récupérées sur le type d'intrusion qui pourrait être réalisé par un hacker en traversant les mécanismes de sécurité informatique.

Les différents tests d'intrusion sont les suivants : Le test en boîte noire, le test en boîte blanche, le test en boîte grise. Les étapes de la réalisation d'un test d'intrusion sont : définir le périmètre de test, le choix de la stratégie ainsi que le type de test d'intrusion, lancer une attaque en fonction du scénario d'attaque choisi, rédiger un rapport.

En effectuant un audit de configuration, vous réalisez une évaluation technique de la configuration des composants du système d'information. En faisant cela, vous vous assurez que les mesures de sécurité respectent bien les bonnes pratiques en matière de sécurité. Une fois l'audit réalisé, le système pourra être durci et sera donc mieux préparé aux attaques. L'audit de configuration n'est qu'une petite partie de la méthode d'audit proposé par l'ANSSI. Ainsi, un audit de configuration doit être complété de différents audits importants pour la mise en sécurité de votre réseau (audit applicatif, de code source, de centre de serveur, d'architecture réseau, organisationnel, etc.).

## VIII. Auto-évaluation

### Exercice 1

[solution n°4 p.15]

#### Trouvez la définition de ces tests :

L'objectif de ce test est d'avoir accès à la totalité des informations sur le système pour le testeur. Il s'agit ici d'une autre vision d'une personne qui serait en possession des mots de passe permettant d'avoir un accès administrateur. Cette approche est celle qui permet de détecter le plus de failles de sécurité.

Ce test consiste à la réalisation d'un test d'intrusion en exploitant la moindre information du réseau. Ce test est réalisé dans des conditions imitant une attaque par un pirate informatique venant de l'extérieur.

Ce test consiste à faire une tentative d'introduction dans un système d'information en disposant seulement de peu d'informations concernant l'organisation du système. Il s'agit donc d'un test simulant une attaque par un client, un prestataire, ou un salarié malhonnête.

**Le test en boîte noire**

**Le test en boîte blanche**

**Le test en boîte grise**

## Exercice 2 : Quiz

[solution n°5 p.16]

### Question 1

Le test d'intrusion est un synonyme du scanner de vulnérabilité.

- ☐ Vrai
- ☐ Faux

### Question 2

Un test d'intrusion permet d'identifier le niveau de sécurité présent dans le Système d'Information.

- ☐ Vrai
- ☐ Faux

### Question 3

Le test de vulnérabilité est une attaque contrôlée.

- ☐ Vrai
- ☐ Faux

### Question 4

Une fois le test d'intrusion réalisé, les administrateurs systèmes et réseaux pourront mettre en place une stratégie leur permettant de sécuriser le réseau.

- ☐ Vrai
- ☐ Faux

### Question 5

Le rapport doit contenir uniquement la liste des vulnérabilités découvertes.

- ☐ Vrai
- ☐ Faux

## Solutions des exercices




**Exercice p. 5 Solution n°1****Question 1**

Un test d'intrusion doit suivre un schéma comportant au minimum 3 étapes.

☐ Vrai

☒ Faux


 Faux. Un test d'intrusion doit suivre un schéma comportant au minimum 4 étapes.

**Question 2**

La deuxième étape d'un test d'intrusion est la plus importante, il s'agit du choix de la stratégie.

☐ Vrai

☒ Faux


 Faux. C'est la troisième étape la plus importante, celle du lancement de l'attaque.

**Question 3**

À la fin du processus, il est primordial de rédiger un rapport.

☒ Vrai

☐ Faux


 Vrai. La quatrième et dernière étape du processus de test d'intrusion est la création d'un rapport.

**Question 4**

Le test d'intrusion interne permet de placer le testeur à l'extérieur du réseau cible.

☐ Vrai

☒ Faux


 Faux. Le test d'intrusion interne permet au testeur d'être directement placé sur le réseau cible.

**Question 5**

Pour améliorer la sécurité de l'entreprise, il est important de mettre en place directement un test d'intrusion.

☐ Vrai

☒ Faux

 Faux. Pour améliorer la sécurité de l'entreprise, il est important de mettre en place différents audits permettant de comprendre l'état dans lequel se trouve le matériel.


**Exercice p. 7 Solution n°2**

### Question 1

Un audit de configuration permet de mettre en évidence les erreurs de sécurité présentes.

☒ Vrai

☐ Faux


 Vrai, il permet de mettre en évidence les erreurs de sécurité présentes et représente donc un fondement essentiel de la cybersécurité.

### Question 2

Il n'y a pas de pré-requis avant de démarrer l'audit.

☐ Vrai

☒ Faux


 Faux, avant de réaliser l'audit, l'auditeur doit avoir récupéré tous les accords nécessaires à la manipulation des données présentes sur les différentes machines du réseau.

### Question 3

En effectuant un audit de configuration, vous réalisez :

☐ Un test de la configuration des composants du système d'information

☒ Une évaluation technique de la configuration des composants du système d'information


 En effectuant un audit de configuration, vous réalisez une évaluation technique de la configuration des composants du système d'information.

### Question 4

Vous devez vérifier uniquement les équipements réseaux, les systèmes d'exploitation.

☐ Vrai

☒ Faux


 Faux. Vous devez vérifier les équipements réseaux, les systèmes d'exploitation, les logiciels, les applications, les bases de données, etc.

### Question 5

Un audit de configuration permet de définir le plan d'action technique à privilégier.

☒ Vrai

☐ Faux

 Vrai, un audit de configuration permet de définir le plan d'action technique à privilégier mais aussi d'évaluer le niveau de sécurité des machines.


## Exercice p. 9 Solution n°3

**Question 1**

L'ANSSI est un organisme privé.

☐ Vrai

☒ Faux


 L'ANSSI est un organisme public qui dépend du Premier Ministre.

**Question 2**

Les employés du service informatique n'ont besoin que d'un compte administrateur.

☐ Vrai

☒ Faux


 Pour effectuer des tâches comme les mails ou la navigation Internet, il est recommandé d'avoir un compte sans privilège.

**Question 3**

Les utilisateurs ne doivent pas avoir de mots de passe en commun.

☒ Vrai

☐ Faux


 Les utilisateurs doivent tous avoir des mots de passe différents.

**Question 4**

Pourquoi les administrateurs doivent-ils utiliser des comptes individuels et personnels pour se connecter aux différentes machines du réseau ?

☐ Pour être organisés

☒ Pour avoir une traçabilité


 Pour avoir une traçabilité, tous les administrateurs doivent disposer d'un compte individuel avec des mots de passe différents.

**Question 5**

Pour vérifier tous les éléments s'étant passés sur le réseau, je dois regarder dans les logs.

☒ Vrai

☐ Faux

 En analysant les journaux, vous pourrez vérifier tous les événements se déroulant, notamment aux heures critiques comme la nuit ou le week-end.

**Exercice p. 10 Solution n°4**

**Trouvez la définition de ces tests :**

**Le test en boîte noire**

Ce test consiste à la réalisation d'un test d'intrusion en exploitant la moindre information du réseau. Ce test est réalisé dans des conditions imitant une attaque par un pirate informatique venant de l'extérieur.

**Le test en boîte blanche**

L'objectif de ce test est d'avoir accès à la totalité des informations sur le système pour le testeur. Il s'agit ici d'une autre vision d'une personne qui serait en possession des mots de passe permettant d'avoir un accès administrateur. Cette approche est celle qui permet de détecter le plus de failles de sécurité.

**Le test en boîte grise**

Ce test consiste à faire une tentative d'introduction dans un système d'information en disposant seulement de peu d'informations concernant l'organisation du système. Il s'agit donc d'un test simulant une attaque par un client, un prestataire, ou un salarié malhonnête.

**Q Le test en boîte noire :** Le test en boîte noire consiste à la réalisation d'un test d'intrusion en exploitant la moindre information du réseau. Ce test est réalisé dans des conditions imitant une attaque par un pirate informatique venant de l'extérieur.

**Le test en boîte blanche :** L'objectif de ce test est d'avoir accès à la totalité des informations sur le système pour le testeur. Il s'agit ici d'une autre vision d'une personne qui serait en possession des mots de passe permettant d'avoir un accès administrateur. Cette approche est celle qui permet de détecter le plus de failles de sécurité.

**Le test en boîte grise :** Ce test consiste à faire une tentative d'introduction dans un système d'information en disposant seulement de peu d'informations concernant l'organisation du système. Il s'agit donc d'un test simulant une attaque par un client, un prestataire, ou un salarié malhonnête.

**Exercice p. 11 Solution n°5**

**Question 1**

Le test d'intrusion est un synonyme du scanner de vulnérabilité.

☐ Vrai

☒ Faux

**Q** Faux. Le test d'intrusion n'est pas non plus à confondre avec le scanner de vulnérabilité.

**Question 2**

Un test d'intrusion permet d'identifier le niveau de sécurité présent dans le Système d'Information.

☒ Vrai

☐ Faux

**Q** Vrai. Un test d'intrusion permet d'identifier le niveau de sécurité présent dans le Système d'Information de l'entreprise.


**Question 3**

Le test de vulnérabilité est une attaque contrôlée.

☒ Vrai

☐ Faux



 Vrai. Il s'agit d'une attaque contrôlée qui révélera le niveau de sécurité actuel.


#### Question 4

---

Une fois le test d'intrusion réalisé, les administrateurs systèmes et réseaux pourront mettre en place une stratégie leur permettant de sécuriser le réseau.

☒ Vrai

☐ Faux

 Vrai. Les administrateurs systèmes et réseaux pourront mettre en place une stratégie leur permettant de sécuriser le réseau en le protégeant face aux attaques éventuelles de personnes mal intentionnées.


#### Question 5

---

Le rapport doit contenir uniquement la liste des vulnérabilités découvertes.

☐ Vrai

☒ Faux

 Faux. Il doit contenir d'autres éléments.