
phosforea
my learning experience

Manager un programme de test d'intrusion des systèmes d'information

-Session Présentielle-

phosforea
my learning experience

Objectifs de la session

- Gérer un programme de tests d'intrusion,
  - Découvrir la méthodologie des tests
  - Découvrir les concepts techniques
- Interpréter le rapport,
- Gérer les actions correctives.

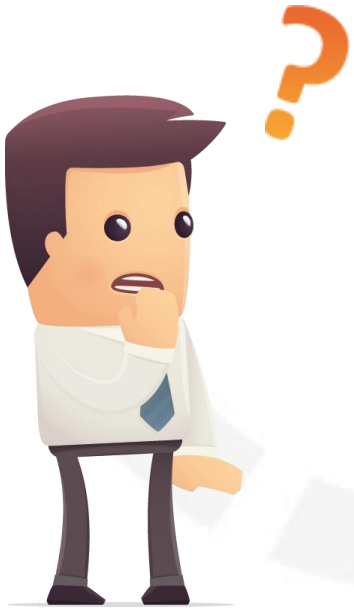
Etude de cas

- Vous êtes responsable de la sécurité du site Web de votre entreprise.
- Votre hiérarchie vous demande de vérifier la sécurité de ce site car cela n'a jamais été fait.
- Vous devez donc réaliser un test d'intrusion de votre système et présenter votre rapport et vos recommandations à votre direction.
- Comment allez-vous procéder ?

Comment procéder ?

Je cherche un plan existant pour repérer mon matériel ?

J'analyse mon système en me connectant sur chaque machine ?



J'appelle un ami...

phosforea
my learning experience

Introduction aux tests d'intrusion

Le test d'intrusion

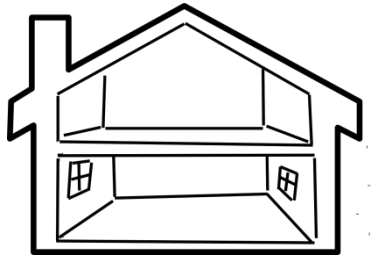
- **Principe** : **découvrir des vulnérabilités** sur le système d'information audité et vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel, le tout **dans un cadre légal**.

- **Objectif principal** : lister les éventuelles vulnérabilités présentes et proposer des contre-mesures.

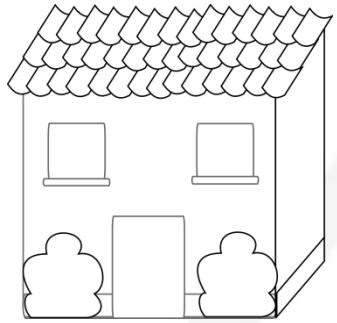
- **Remarque** : **un test d'intrusion seul n'a pas vocation à être exhaustif**. Il peut, en effet, être réalisé en complément d'autres audits (en général, audit de code) afin d'en améliorer l'efficacité ou de vérifier l'exploitabilité d'une vulnérabilité.

2 types de tests d'intrusion

- Tests d'intrusion internes :
  - Cela signifie que les tests sont réalisés directement depuis l'intérieur de l'entreprise (en général dans ses locaux).
  - Avantage : pouvoir écouter ou interagir avec le réseau de l'entreprise.
  - Inconvénient : on considère que l'attaquant est déjà dans l'entreprise.



- Tests d'intrusion externes :
  - Cela signifie que les tests sont réalisés depuis un poste externe à l'entreprise
  - Avantage : mise en situation plus réaliste par rapport à des attaques potentielles.



Les objectifs d'un test d'intrusion

Plusieurs objectifs pour l'entreprise :

1. Détecter les vulnérabilités et donner leurs caractéristiques (facilité d'exploitation, impact, niveau de risque, priorité)
2. Lister les contre-mesures pour se protéger de ces vulnérabilités
3. Fournir un rapport de test d'intrusion pour la traçabilité
4. Proposer un plan d'action de correction des vulnérabilités

Que faire AVANT le test d'intrusion ?

1. Définir la cible et le périmètre
2. Choisir son environnement
3. Décider s'il faut imposer des limites
4. Définir quels types de tests doivent être réalisés et pourquoi

phosforea
my learning experience

Définir la cible

Avant de commanditer un test d'intrusion, il faut savoir sur quoi faire les tests !

Quelques questions à se poser :

- ✓ Quelles sont les fonctions ou données les plus critiques ?
- ✓ Quoi cibler : serveurs, postes de travail, réseau … ?
- ✓ Quelles sont les fonctions de ces biens (serveur de fichier, site internet / intranet …) ?
- ✓ Est-ce le bon moment pour faire les tests (évolutions prévues ...) ?

Définir la cible

Exemple pour un site Web, plusieurs points à vérifier :

- Site commercial ? Intranet ?
- Combien de pages ? De fonctionnalités ?
- Combien de formulaires ?
- Présence d'une authentification d'utilisateurs ?
- Quel langage est utilisé ?
- Quelle adresse IP est concernée ?
- Qui est l'hébergeur ?

Définir la cible

Exemple pour un réseau interne :

- Quelles plages d'adresses IP ?
- Quels sont les serveurs les plus critiques ?
- Quel est l'impact sur les utilisateurs en cas de test d'intrusion sur ces serveurs critiques ?
- Cibler les postes utilisateurs ?
- Autoriser le brute-force des comptes ?
- Réseau filaire ? Wifi ?

Définir le périmètre

Pour un serveur Web par exemple, sur quel périmètre faire le test d'intrusion ?

- Quelles pages / fonctions adresser :
  - Les tests doivent-ils prendre en compte les pages nécessitant une authentification ?
  - Des pages sont-elles à exclure du périmètre des tests ?
- Production :
  - Le site de production peut-il être ciblé sans problème ?
  - Possédez-vous un site de développement ?
- Développement :
  - Le site de production est trop critique, il ne doit pas être testé
  - Vous êtes certains que le site de production est identique au site de développement

Définir le périmètre : les exclusions

- Il est parfois nécessaire de préciser que certains tests ne sont pas autorisés.

- Par exemple :
  - Si vous ne souhaitez pas tester la robustesse aux dénis de service => interdire les dénis de service
  - Si vous ne souhaitez pas que les mots de passe soient découverts => interdire les brute-force
  - Si vous ne souhaitez pas que certaines machines soient scannées => interdire le scan de ports

Les acteurs d'un test d'intrusion

- Plusieurs personnes sont impliquées dans un test d'intrusion.
  - Côté audité :
    - La direction qui souhaite évaluer l'état de sécurisation de l'entreprise
    - Le commanditaire (RSSI) qui doit sécuriser l'entreprise
    - Les aides techniques (développeurs, ingénieurs système et réseau, etc.) qui participent à la sécurisation des systèmes
    - Les utilisateurs de la cible qui peuvent être potentiellement impactés
  - Côté auditeur :
    - Le chef de projet qui va organiser les tests selon un planning
    - Le ou les consultants en sécurité (auditeurs) qui effectueront le test d'intrusion
    - Le commercial qui va donner un tarif selon les demandes dans le cas de sous-traitance externe

La planification

- Il est important de savoir à quel moment réaliser le test d'intrusion.

- Dans quels cas un test d'intrusion est préférable ?
  - Vous devez livrer une nouvelle version de votre application
  - Vous avez été mandaté pour créer un site Web
  - Votre hiérarchie pense que le réseau interne a été compromis

Gestion d'un programme de test d'intrusion

phosforea
my learning experience

1. Les types de tests

Tests en boite noire

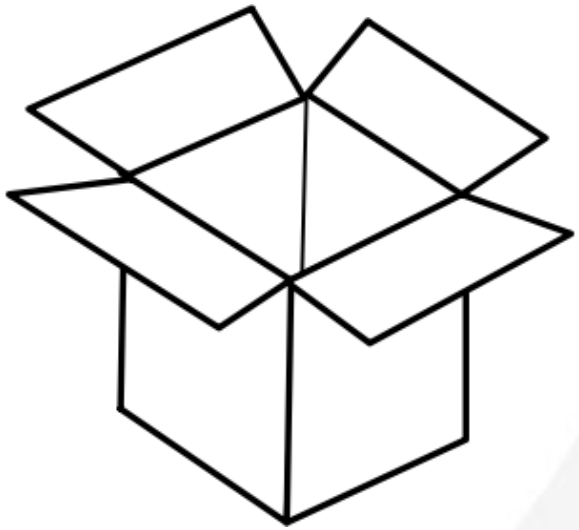
- Un test en boîte noire signifie que le test est réalisé sans aucune connaissance préalable de l'environnement par l'auditeur.

- Avantages :
  - Les tests sont réalisés dans les mêmes conditions qu'un attaquant.

- Inconvénients :
  - Certaines vulnérabilités ne peuvent pas être détectées

Tests en boite blanche

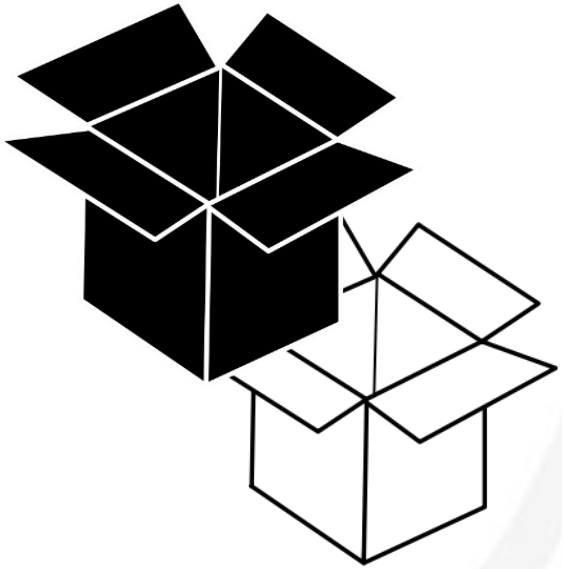
- Un test en boîte blanche signifie que le test est réalisé avec une connaissance totale de l'environnement par l'auditeur (code source, architecture technique, paramètres, etc.)



- Avantages :
  - De nombreuses vulnérabilités peuvent être découvertes du fait de la couverture de l'ensemble des composants
- Inconvénients :
  - Non représentatif d'une intrusion réelle
  - Plus long et donc plus coûteux

Tests en boite grise

- Il s'agit ici d'un mélange de boîte noire et blanche, c'est-à-dire que l'auditeur réalise le test d'intrusion en boîte noire mais en ayant connaissance de certaines informations, par exemple des comptes utilisateurs (login/mot de passe).



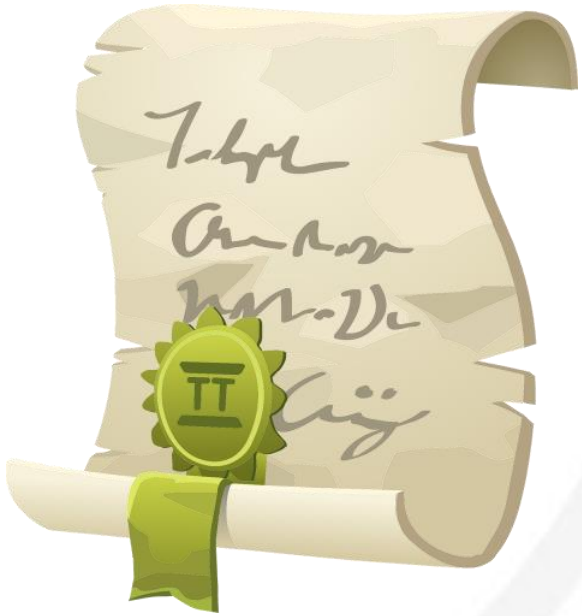
- Avantages :
  - Certaines parties du périmètre seront accessibles et pourront être auditées.
  - Permet de simuler une attaque interne.

- Inconvénients :
  - Un attaquant n'a pas forcément connaissance de ces informations.

2. Le contrat de test d'intrusion

Contrat de TI

- Avant le début d'un test d'intrusion, il convient de signer un contrat avec le prestataire d'audit mandaté pour réaliser l'audit
- Ce contrat devra prendre en compte l'ensemble des législations en vigueur (détaillées ultérieurement).
- Seul l'accord explicite de l'audité permettra de commencer les tests d'intrusion.



Contrat de TI

- Règle de base : qualité du rapport et des conseils, détails des vulnérabilités et de leurs contre-mesures.
- Il permet de définir les conditions et le contexte dans lesquels sont effectués les tests.
- Il fournit une preuve d'un point de vue légal si nécessaire.

Contrat de TI

Ce document contient les informations suivantes :

3. Cadre juridique

phosforea
my learning experience

Le secret professionnel de l'auditeur

- Une clause de confidentialité est généralement signée par l'audité et le prestataire d'audit, ce qui permet d'encadrer la façon dont les informations seront échangées ou encore la manière de travailler.
- Signature d'un NDA (*Non-Disclosure Agreement*) : Accord de non-divulgation des informations d'un projet entre deux entités.
- L'auditeur est tenu de ne jamais révéler d'informations à un tiers, car elles pourraient compromettre la société auditée.

Cadre juridique

- L'article 323 du code pénal est applicable aux intrusions dans des systèmes d'information.
- Article 323-1 :
  - « Le fait d'accéder ou de se maintenir, **frauduleusement**, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et 30 000 euros d'amende.
  - Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende. »
- Un **Système de traitement automatisé de données (STAD)** est une notion très large regroupant n'importe quel système d'information.
- La **tentative d'intrusion** (échec de l'intrusion) est punie des **mêmes peines** que l'accès réussi.

Cadre juridique

aucune autorisation = fraude

autorisation = pas de fraude !

- Il est donc important de garder une **preuve** de l'accord explicite signé entre l'auditeur et l'audité avant, pendant et après l'audit.

phosforea
my learning experience

Référentiel de l'intrusion

- En 2012, la Fédération des Professionnels des Tests Intrusifs (F.P.T.I.) publie une charte de l'intrusion à destination des professionnels réalisant des tests d'intrusion.
- Les professionnels n'ont **aucune obligation** de suivre ce référentiel mais il peut être utile.
- Le référentiel de l'intrusion est composé de 3 éléments :
  1. Les principes fondateurs
  2. La charte de l'intrusion
  3. La démarche de l'intrusion

- Plus de détails sur : http://www.fpti.pro/

phosforea
my learning experience

Référentiel de l'intrusion

- Les principes fondateurs de la **F.P.T.I.** se traduisent par **11 règles professionnelles** encadrant la pratique des tests d'intrusion, en voici quelques-unes :
  - Le Professionnel ne peut prétendre être exhaustif dans l'inventaire des différents moyens de s'introduire sur les cibles, sauf à disposer de ressources illimitées (en moyens humains, en durée de prestation, ...).
  - Le Professionnel prestataire de service a souscrit à une **assurance civile et professionnelle** couvrant les dommages éventuellement causés dans le cadre d'un test d'intrusion.
  - Le Professionnel s'engage à adopter une **approche basée sur la preuve** pour parvenir à des conclusions fiables et reproductibles.

Charte de l'intrusion

- La Charte de l'Intrusion énonce le code déontologique de la Profession. Elle a aussi été créée par la FPTI.

- Elle contient 10 articles articulés autour de 4 principes :
  1. Principe de moralité
  2. Principe de transparence
  3. Principe de confidentialité
  4. Principe de probité

La démarche de l'intrusion

- La démarche de l'intrusion comprend 3 phases :
  1. Phase d'initialisation : valider le périmètre, les rôles de chacun, etc.
  2. Phase de test : réalisation des scénarii d'attaques
     - Découverte de la cible
     - Recherche de vulnérabilités
     - Intrusion
  3. Phase de restitution : livrable, présentation des résultats

Respecter la vie privée des utilisateurs

- **« Chacun a droit au respect de sa vie privée »** comme le stipule le code civil (article 9 datant de 1970). La CNIL est chargée de cette tâche.

- Toutes les traces / preuves qui auront été relevées pendant le test d'intrusion doivent être stockées chiffrées et communiquées aux seules personnes responsables prévues dans le contrat avec l'auditeur.

Par exemple, en cas de diffusion publique d'une photo d'un collaborateur dans un lieu privé, le code pénal prévoit (article 226-1) :

1 an d'emprisonnement et 45 000 € d'amende pour celui qui a diffusé.

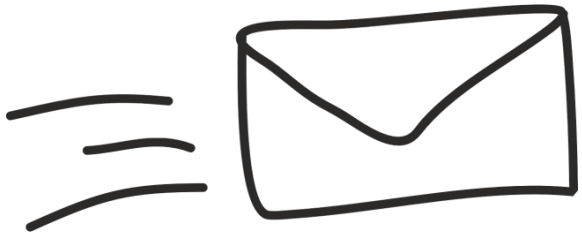
La police du respect de la vie privée : la CNIL

- La Commission Nationale de l'Informatique et des Libertés (CNIL) a été créé en 1978 et a pour mission de protéger les données personnelles en France.
- Elle veille à ce que les entreprises respectent les lois concernant le respect de la **vie privée** (au niveau informatique, Internet ou non).
- Elle est indépendante et a un pouvoir de sanction pour les fautifs.
- 174 agents ont réalisé plus de 450 contrôles en 2014.
- Elle dispose d'un budget de 16 millions d'euros.
- http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

CNIL

Le secret des correspondances

- Le code pénal prévoit aussi de sanctionner l'atteinte au secret des correspondances (article 226-15) :
  - « Le fait, commis de mauvaise foi, **d'ouvrir, de supprimer, de retarder ou de détourner des correspondances** arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
  - Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues **par la voie électronique** ou **de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions**.»



La convention d'audit

- La convention d'audit est un document formel encadrant la réalisation des test d'intrusion, signé entre l'auditeur et l'audité

- La convention d'audit peut se substituer si nécessaire au contrat d'audit

- Cette convention contient notamment :
  - L'identification des parties intéressées,
  - Le rappel des objectifs et du contexte de réalisation,
  - Les modalités de réalisation de la mission (lieux, matériels, outils, règles, échange d'information…),
  - La définition du périmètre ciblé, des limites et exclusions éventuelles
  - Un rappel sur les risques d'audit
  - Le planning et les jalons
  - La description des livrables
  - Le cadre juridique applicable

4. Etapes d'un test d'intrusion

Les étapes d'un test d'intrusion

- Il n'y a pas de guide officiel mais nous considérons généralement 3 phases dans la réalisation d'un test d'intrusion :

Cette phase est réalisée en 3 étapes :

C'est cette étape-ci que nous détaillerons dans ce module

1. Découverte de la cible : collecter des informations sur le périmètre cible
2. Recherche de vulnérabilités : identifier des vulnérabilités sur les cibles
3. Intrusion : exploiter les vulnérabilités

La phase d'initialisation

- Cette phase permet de :
  - Présenter les intervenants, rôles, responsabilités
  - Valider les aspects contractuels et législatif relatifs au test
  - Valider le périmètre et les scénarios du test
  - Préciser les conditions particulières du test
  - Communiquer les informations techniques
  - Définir les moyens de communications entre les intervenants

La phase d'initialisation

- Concrètement, vous devez :
  - Préparer une réunion d'initialisation avec tous les intervenants
  - Définir et rédiger les objectifs
  - Définir et rédiger le périmètre cible
  - Connaître les noms, les versions des serveurs et ce qu'ils contiennent

phosforea
my learning experience

La phase de test

- Cette phase est réalisée en 3 étapes :
    1. Découverte de la cible : collecter des informations sur le périmètre cible
    2. Recherche de vulnérabilités : identifier des vulnérabilités sur les cibles
    3. Intrusion : exploiter les vulnérabilités

- L'auditeur s'appuie sur des outils divers (auto développement, sous licence…) pour la réalisation des différentes phases

La phase de restitution

- Cette phase permet de rendre compte au demandeur de l'état des lieux du niveau de sécurité du périmètre ciblé.
- Le livrable contient notamment :
  - La liste des vulnérabilités identifiées et exploitées
  - La liste des contre-mesures associées
- Ce document doit contenir suffisamment d'informations pour permettre aux responsables et aux développeurs de comprendre les problèmes identifiés et les mesures à prendre pour les corriger.

Suivre le déroulement d'un test d'intrusion

phosforea
my learning experience

Objectif

- Etre capable d'assurer le suivi d'un test d'intrusion
- Traiter les résultats au travers de l'interprétation du rapport d'audit
- Mettre en œuvre des actions correctives et préventives adaptées

phosforea
my learning experience

Synchronisation entre audités et auditeurs

phosforea
my learning experience

La synchronisation

- Un contact doit être maintenu durant toute la durée de l'audit entre l'audité et l'auditeur, un personnel interne a l'organisation doit donc être désigné et disponible (en général le RSSI) pour :
  - Traiter la découverte de vulnérabilités critiques (procédure d'urgence durant les pentests)
  - Traiter les éventuels points de blocage (comptes invalides, réseaux fermés, agendas…)
  - Assurer la communication interne à l'organisation et fournir les informations nécessaires à l'auditeur si cela est requis

- Des points quotidiens sont à prévoir avec les auditeurs pour cela

La synthèse « à chaud »

- Pourquoi faire une synthèse quotidienne entre l'audité et l'auditeur ?
  1. Pour s'assurer de la tenue des plannings (réalisé VS reste à faire) et ajuster si nécessaire le plan d'audit
     - Liste des tests réalisés / non réalisés,
     - Liste des tests prévus / annulés
  2. Pour échanger sur les vulnérabilités détectées durant l'audit
     - Estimation commune des impacts,
     - Echanges sur les corrections et actions correctives
  3. Pour échanger sur le déroulement global
     - Participation des audités,
     - Point de blocage, difficultés …

phosforea
my learning experience

Procédure d'urgence

- Pour rappel : une vulnérabilité critique est une vulnérabilité dont l'exploitation est aisée et les impacts élevés pour l'organisation

- Un traitement doit donc être apporté au plus vite, au regard du risque pour l'organisation
  1. Par suppression de la vulnérabilité (patch par exemple)
  2. Par suppression de l'exposition ou des moyens d'exploitation (débrancher du réseau)
  3. Ou tout simplement accepter le risque et envisager un traitement ultérieur

- **Attention** : les impacts de toute action doivent être estimés et validés par l'organisation (coupure de service, restriction d'accès, suppression d'informations…)

phosforea
my learning experience

Gérer les résultats d'un test d'intrusion

phosforea
my learning experience

Le rapport

- A l'issue de la réalisation des tests d'intrusion, l'auditeur remet à l'audité un rapport de tests, devant permettre à l'organisation
  - De prioriser le traitement des risques
  - D'identifier les mesures nécessaires à leur traitement
  - D'engager les ressources pour la mise en œuvre de ces mesures
  - De planifier leur mise en œuvre

Deux types de rapport

- **Rapport technique détaillé**, à destination des personnels technique, permettant de décrire pour chaque vulnérabilité
  - Les méthodes d'attaque utilisées,
  - Une estimation de l'exposition de la vulnérabilité,
  - Une estimation de leur gravité / niveau d'impact,
  - Idéalement, les recommandations pour leur traitement

- **Rapport de synthèse** (ou executive summary) à destination des décideurs, utilisé principalement
  - Pour partager à un niveau décisionnel sur les risques existants,
  - Pour présenter une évaluation du niveau de sécurité du périmètre audité,
  - Pour permettre de décider de l'application d'un plan d'action,
  - Pour convaincre de la nécessité de sécurisation …

Spécificités d'un rapport de Pentest

- Compte tenu de la nature sensible du contenu du document (explications détaillées sur les points sensibles d'une organisation), il est fortement conseillé de traiter ce document comme un document **confidentiel entreprise**.
- Les modalités d'échange et les destinataires de ce rapport devant alors être précisées initialement (idéalement dans la convention ou le contrat d'audit)
- L'audité est responsable de la diffusion qui en est faite à l'intérieur de l'organisation
- L'auditeur doit en gérer strictement la confidentialité

phosforea
my learning experience

Structure d'un rapport

Un rapport de test d'intrusion inclut généralement les éléments suivants :

- Rappel du contexte et des objectifs
- Rappel du périmètre / des cibles et des modalités de tests
- Rappel des risques d'audit
- Présentation des auditeurs
- Identification des parties intéressées
- Description des tests réalisés
- Description des vulnérabilités et des recommandations détaillées
- Synthèse générale incluant :
  1. Une évaluation globale
  2. Une synthèse des vulnérabilités
  3. Une synthèse des recommandations
- Annexes éventuelles

Le contexte et les objectifs

- Pourquoi l'audit a t'il été commandité ?
- Qui est à l'origine de la demande ?
- Quelle a été la période de réalisation ?
- Quels sont les objectifs ?
  1. Quelles informations sont attendues ?
  2. A quoi vont-elles servir ?

phosforea
my learning experience

Le périmètre des tests

- Exemple de rapport détaillant le périmètre des tests d'intrusion

2.1 PRESENTATION DU PERIMETRE

Les tests de vulnérabilités et d'intrusion ont été réalisés les JJ/MM/2015 et JJ/MM/2015 pour les tests d'intrusion.

L'architecture est composée des éléments suivants :

Périmètre		
Nom de la cible	**URL**	**Adresse IP**
Site public	https://xxxxxxxxxxxx.com	A.B.C.D
Accès interne	https://yyyyyyyyyyy.com	A.B.C.D

Les tests se sont déroulés :

- En boite noire (accès sans compte ni information particulière)
- En boite grise (fourniture de comptes avec login et mot de passe d'accès à l'application) :
  - Cartographie des services de l'application
  - Recherche et exploitation de vulnérabilités
- En boite blanche (fourniture des fichiers de configuration, accès au serveur par VPN) :
  - Analyse des fichiers de configuration

NB : Il est rappelé que les tests en boîte noire et grise sur une durée limitée permettent une évaluation

Les risques d'audit

- Il convient de rappeler dans le rapport les différents risques liés à l'audit, d'une manière générale :
  - Risques de non détection
  - Non-Exhaustivité des tests
  - Impacts sur l'environnement technique
- Ces risques d'audits peuvent être :
  - Du fait de l'auditeur,
  - Du fait de l'environnement technique,
  - Du fait du temps consacré à la réalisation des tests pour chaque cible,
  - Du fait des tests à réaliser et convenus initialement,
  - Du fait de manque d'information

Les auditeurs

- Le rapport d'audit doit permettre l'identification du/des auditeurs et préciser leur coordonnées
  - Pour questions ultérieures,
  - Pour contrôle de référence,
  - Pour la traçabilité

1.1 AUDITEURS

Prénom NOM	Coordonnées (email)	Fonction
Auditeur 1	auditeur.un@societe.com	Chef de projet / Lead pentester
Auditeur 2	auditeur.deux@societe.com	Pentesteur Web
Auditeur 3	Auditeur.trois@societe.com	Pentesteur Web + Infra

Les parties intéressées

- Le rapport d'audit doit également rappeler qui sont les parties intéressées, et leur rôle dans le projet

1.2 PARTIES INTERESSEES INTERNES

Prénom NOM	Coordonnées (email)	Fonction
Mister Pink	pink@target.com	Commanditaire
Miss Blue	blue@target.com	Directrice informatique
Mister Grey	grey@target.com	Administrateur système
Mister White	white@target.com	Développeur
Miss Yellow	yellow@target.com	Observatrice

Les tests réalisés

- Une synthèse des tests réalisés doit permettre à l'audité de déterminer si la couverture des tests est suffisante au regard des objectifs de mission, et permet une appréciation générale du niveau de qualité de la prestation

- Des résultats préliminaires peuvent si besoin être présentés

Test de la gestion de configuration	Chiffrement SSL/TLS	*Le chiffrement des connexions peut présenter des faiblesses si la version SSL, les algorithmes, la longueur de clés ou la validité du certificat sont mal paramétrés.* Le protocole TLS 1.2 n'est pas supporté.
	Gestion des fichiers	*Il est possible de lister les fichiers stockés dans les répertoires si le serveur n'est pas durci.* Les répertoires ne peuvent pas être listés.
	Fichiers anciens, sauvegardes	*Les fichiers de sauvegarde ou les fichiers d'anciennes versions peuvent fournir des informations sensibles.* Aucun fichier ancien ou de sauvegarde n'a été découvert.
	Présence d'interfaces d'administration	*Les interfaces d'administration sont une cible privilégiée pour prendre le contrôle d'un site WEB.* Aucune trouvée.
	Test des méthodes HTTP supportées	*Certaines méthodes HTTP permettent de lancer des attaques contre le site WEB et doivent donc être désactivées.* Les méthodes HTTP suivantes sont supportées : GET, POST, PUT, DELETE.
	Transport des données de connexion sur un canal chiffré	*Les données d'authentification doivent transiter par des canaux chiffrés.* Les protocoles TLS 1.1 et 1.2 ne sont pas supportés.
	Découverte de compte utilisateur	*Il est parfois possible de deviner le nom des comptes utilisateurs, en se basant sur les messages d'erreur par exemple.* Il n'a pas été possible de découvrir des comptes utilisateur.
	Découverte de mot de passe par force brute	*En l'absence de protection contre les tentatives de brute-force, il est possible de deviner les mots de passe des comptes utilisateurs.* Aucun mot de passe n'a été découvert.

phosforea
my learning experience

Synthèse générale

- Il s'agit principalement dans ce chapitre du rapport de donner une vision non technique et synthétique des résultats au travers par exemple:
  - D'une évaluation générale de la cible,
  - Du nombre de vulnérabilités par type / criticité,
  - D'une synthèse des risques encourus par la cible
  - D'une synthèse des recommandations (sous la forme de plan global)

D'après les tests réalisés, le niveau de sécurité de l'application XXXXX est globalement évalué à **FAIBLE**. Les tests réalisés ont révélé un total de **10** vulnérabilités réparties selon les niveaux de criticité suivants :

- 0 vulnérabilité de criticité **mineure ;**
- 0 vulnérabilité de criticité **importante ;**
- 8 vulnérabilités de criticité **majeure ;**
- 2 vulnérabilités de criticité **critique**.

L'exploitation de ces vulnérabilités peut conduire aux scénarios d'attaques et de menaces suivants :

- Un utilisateur authentifié peut exécuter des requêtes SQL
- Un utilisateur authentifié peut modifier son rôle pour élever ses privilèges
- Un utilisateur authentifié peut lire des contrats en dehors de son arborescence
- Un utilisateur authentifié peut lire des appels en dehors de son arborescence

Ces scénarios peuvent engendrer les conséquences suivantes pour la cible :

- Vol de toute la base de données accessible
- Lecture de contrats et d'appels appartenant à d'autres entités
- Lecture, modification et suppression de toute l'arborescence en tant qu'utilisateur administrateur

Afin d'atténuer ces risques, les recommandations suivantes doivent être appliquées :

- Restreindre les caractères autorisés pour les requêtes SQL
- Restreindre les fonctions de recherche à l'arborescence descendante (accès uniquement aux fils)
- Vérifier les autorisations pour chaque action notamment lors de la modification des rôles

Les vulnérabilités

- Chaque vulnérabilité doit être présentée précisément et préciser son impact, son exploitabilité (parfois au travers d'une probabilité d'occurrence) et une estimation des risques liés
- Un scénario d'attaque peut être présenté afin de faire comprendre à des non spécialistes le problème.
- Un PoC (*Proof of Concept*), ou à minima la méthode d'exploitation, doit être détaillé afin de pouvoir si besoin rejouer le test et valider plus tard sa correction.
- Des contre-mesures doivent être proposées.

Exemples de fiche de vulnérabilité

DEV-01	**Interface d'administration des news accessible sans mot de passe**	**Niveau de risque :** CRITIQUE
Constats	La page d'administration /admin/admin.php est accessible sans identification et authentification. Seul le dernier bouton permettant l'administration des news renvoi sur une page fonctionnelle : 

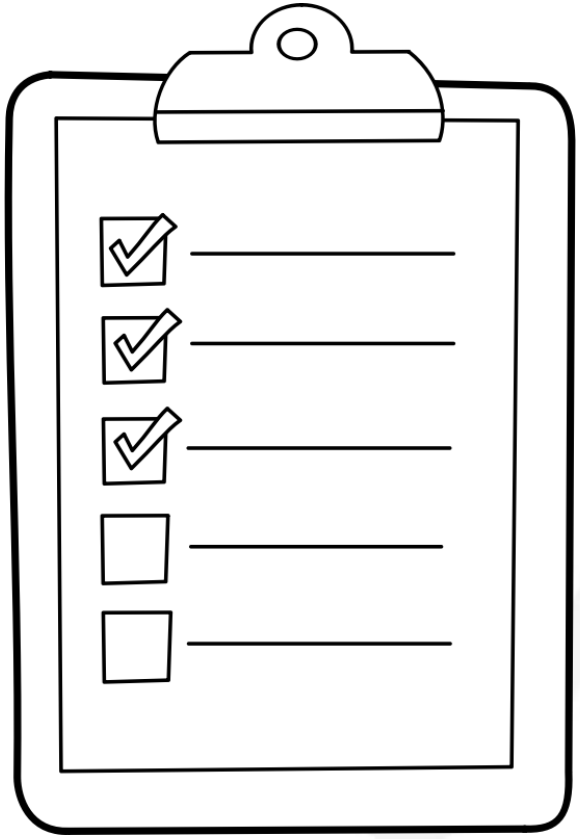
phosforea
my learning experience

Exemples de fiche de vulnérabilité

Exploitation	Les news peuvent au travers de cette page être éditées ou supprimées	
Risques	La disponibilité des news ainsi que leur intégrité peuvent ainsi être affectées, un attaquant pouvant ainsi au travers de cette vulnérabilité mettre en danger l'organisation en véhiculant des messages illicites (incitation à la haine, dénigrement d'entreprises ou de personnes, message partisan, etc.)	
Facilité d'exploitation : Facile		**Impact :** Critique
Recommandations	**Actions correctives** AC1 : Ne pas rendre publique ces pages d'administration. Protéger l'accès par un mécanisme d'authentification.	
Charge de mise en œuvre des recommandations : moyenne		**FAIBLE**

Les annexes

- Les annexes doivent contenir tout ce qui peut aider à comprendre les vulnérabilités :
  - Captures d'écrans
  - Scripts développés ou utilisés pour l'exploitation (par exemple un script Metasploit que l'on aurait développé)
  - Trames réseaux
  - Détail du retour d'un scan
  - Détail des vulnérabilités donné par les outils utilisés tels que OpenVAS ou Nikto



Interpréter les recommandations et mettre en œuvre le plan d'action correctif

phosforea
my learning experience

Les recommandations

- Un ensemble de recommandations doivent être énoncées dans le rapport d'audit

- On distingue trois types de recommandations :
  1. Les corrections
     - Il s'agit de mesures permettant de traiter les effets d'une vulnérabilité
  2. Les actions correctives
     - Il s'agit de mesures visant à éliminer les causes racines d'une vulnérabilité
  3. Les actions préventives
     - Ces mesures visent à éviter l'apparition d'une vulnérabilité suspectée

Les recommandations

- Considérons par exemple, le constat suivant : « Serveur apache dans une version obsolète »
- La correction consiste alors à patcher le serveur dans la dernière version non vulnérable,
- La mesure corrective vise en revanche à doter l'organisation d'un processus de gestion des vulnérabilité logicielle
  - Cela pourrait être une mesure préventive si le serveur était à jour car fraîchement installé, mais que l'auditeur ait constaté l'absence de ce type de processus

Les recommandations

Les recommandations peuvent être de plusieurs natures :

- **Techniques** : consiste en des actes techniques sur le SI
  - Ex: Reconfigurer le firewall
- **Organisationnelles** : touche à la structure de l'organisation
  - Ex: nommer un RSSI
- **Managériales** : consignes applicables
  - Ex : ne plus utiliser de logiciels non validés par la DSI
- **Physiques** : applicable à l'environnement
  - Ex: séparer les équipes de DEV et de PROD

Les recommandations

Il convient pour l'organisation d'établir un plan d'action qui lui est propre sur la base de l'ensemble des recommandations formulées

Pour chaque action prévue, il sera alors nécessaire de:

- Estimer la charge et le coût de mise en œuvre (des estimations peuvent avoir été formulées par les auditeurs),
- Evaluer l'effet sur le traitement des risques existants,
- Définir une date d'échéance,
- Identifier le responsable de l'action,
- Estimer les impacts éventuels sur l'organisation
- Définir une priorité de traitement sur la base des éléments précédents

Les vulnérabilités les plus critiques doivent faire l'objet de traitement prioritaire

Les recommandations

A chaque recommandation, une conséquence :

1. Modification d'un fichier de configuration
   - ➢ Peut impliquer un redémarrage du serveur
2. Suppression de fichiers
   - ➢ Fichier utile à quelqu'un ?
3. Modification du code source
   - ➢ Nécessite des tests unitaires
4. Modification de droits sur un fichier
   - ➢ Opération volontaire ou non ?

Préparer un plan d'action correctif

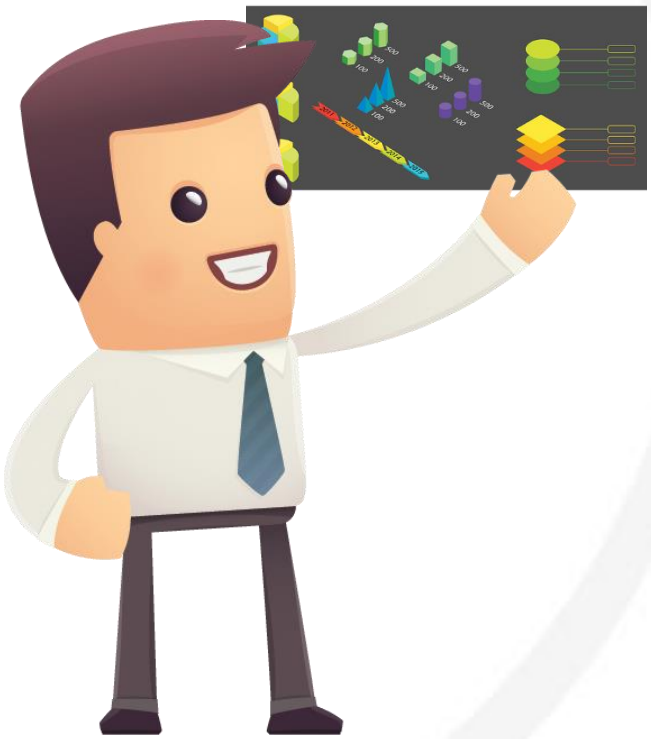
- La mise en œuvre du plan d'action correctif doit donc s'effectuer conformément aux critères établis
  1. Priorité de traitement de l'action,
  2. Planification en tenant compte de l'échéance prévue

- Le responsable de l'action se doit de fournir les ressources nécessaires à leur mise en œuvre et rend compte à la Direction (ou au RSSI selon les cas) de l'avancement des actions.

phosforea
my learning experience

Suivre les corrections

- Une fois les mesures mises en œuvre, il convient de s'assurer de leur bonne implémentation et de leur bon fonctionnement
- Le suivi des corrections doit faire parti de la « Gestion de projet » du produit, les vulnérabilités peuvent être traitées comme des bugs à corriger.
- On veillera en particulier suite à un tests d'intrusion à vérifier que l'exploitation des vulnérabilités détectées devienne « impossible »



Vérifier la mise en place des correctifs

- Le contrôle des vulnérabilités techniques s'effectue la plupart du temps par le rejeu des scénarios d'exploitation des vulnérabilités ayant permis leur découverte

- Cela peut être fait par un prestataire (souvent celui qui a réalisé le test initial, auquel cas il sera nécessaire de prévoir cette phase lors du contrat) ou par les équipes interne sur la base du rapport technique détaillé.

Les effets de bords possibles

- Lors de corrections de vulnérabilités, veillez à ne pas introduire de nouvelles vulnérabilités !
- Exemple :
  - Protéger un fichier par mot de passe est efficace mais seulement si ce mot de passe est complexe sinon il peut être trouvé facilement par un attaquant.
  - Dans ce cas la vulnérabilité « authentification sans mot de passe possible » devient « mot de passe facile à trouver »

Les effets de bords possibles (suite)

- Autre exemple :
  - Il est parfois possible de croire qu'une vulnérabilité est corrigée mais qui est encore présente.
  - Les injections SQL sont souvent **difficiles à corriger** :
    - Ce n'est pas parce que la requête tentée ne fonctionne pas qu'il est impossible d'injecter dans la requête SQL
    - De nombreux exemples existent pour contourner les protections en utilisant des encodages, sans guillemets, sans espaces, etc.

Fin du module

Ce module est à présent terminé, vous pouvez retourner sur votre tableau de bord.

phosforea
my learning experience