Try Hack Me

INTRODUCTION TO PENTESTING

Teste d'intrusions informatique

08 août 2022

By PLarox

Pentesting Fundamentals

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

Avant de vous enseigner les aspects techniques pratiques du piratage éthique, vous devrez en savoir plus sur les responsabilités professionnelles d'un testeur d'intrusion et sur les processus suivis lors de la réalisation de pentest (recherche de vulnérabilités dans une application ou un système client).

L'importance et la pertinence de la cybersécurité ne cessent de croître et peuvent se retrouver dans tous les domaines de la vie. Les gros titres remplissent nos écrans, signalant encore un autre piratage ou une fuite de données.

La cybersécurité est pertinente pour toutes les personnes dans le monde moderne, y compris une politique de mot de passe solide pour protéger vos e-mails ou pour les entreprises et autres organisations qui ont besoin de protéger à la fois les appareils et les données contre les dommages.

Un test d'intrusion ou pentest est une tentative éthique de tester et d'analyser les défenses de sécurité pour protéger ces actifs et informations. Un test d'intrusion implique l'utilisation des mêmes outils, techniques et méthodologies qu'une personne malveillante utiliserait et est similaire à un audit.

Selon Security Magazine , un magazine de l'industrie de la cybersécurité, il y a plus de 2 200 cyberattaques chaque jour - 1 attaque toutes les 39 secondes.

Éthique des tests d'intrusion

La bataille de la légalité et de l'éthique dans la cybersécurité, sans parler des tests d'intrusion, est toujours controversée. Des étiquettes comme "hacking" et "hacker" ont souvent des connotations négatives, en particulier dans la culture pop, grâce à quelques brebis galeuses. L'idée d'accéder légalement à un système informatique est un concept difficile à saisir - après tout, qu'est-ce qui le rend légal exactement ?

Rappelons qu'un test d'intrusion est un **audit autorisé** de la sécurité et des défenses d'un système informatique tel que convenu par les propriétaires des systèmes. La légalité de la pénétration est assez claire dans ce sens ; tout ce qui ne relève pas de cet accord est réputé non autoriser.

Avant le début d'un test d'intrusion, une discussion formelle a lieu entre le testeur d'intrusion et le propriétaire du système. Divers outils, techniques et systèmes à tester sont convenus. Cette discussion **constitue le champ d'application de l'accord de test d'intrusion** et déterminera le déroulement du test d'intrusion.

Les entreprises qui fournissent des services de tests d'intrusion sont tenues de respecter les cadres juridiques et l'accréditation de l'industrie. Par exemple, le National Cyber Security Center (NCSC) a le système d'accréditation CHECK au Royaume-Uni. Cette vérification signifie que seules *"les entreprises agréées [CHECK] peuvent effectuer des tests d'intrusion autorisés sur les systèmes et réseaux du secteur public et de la CNI". (NCSC).*
L'éthique est le débat moral entre le bien et le mal ; là où une action peut être légale, elle peut aller à l'encontre du système de croyances du bien et du mal d'un individu.

Les testeurs d'intrusion seront souvent confrontés à des décisions potentiellement moralement discutables lors d'un test d'intrusion. Par exemple, ils accèdent à une base de données et se voient présenter des données potentiellement sensibles. Ou ils effectuent peut-être une attaque de phishing contre un employé pour tester la sécurité humaine d'une organisation. Si cette action a été convenue au cours des étapes initiales, elle est légale, mais éthiquement discutable.

Les pirates sont classés en trois chapeaux, où leur éthique et leurs motivations derrière leurs actions déterminent dans quelle catégorie de chapeau ils sont placés. Couvrons ces trois dans le tableau ci-dessous:

Catégorie de chapeau	La description	Exemple
Chapeau blanc	Ces pirates sont considérés comme les "bonnes personnes". Ils respectent la loi et utilisent leurs compétences au profit des autres.	Par exemple, un testeur d'intrusion effectuant un engagement autorisé sur une entreprise.
Chapeau gris	Ces personnes utilisent souvent leurs compétences au profit des autres ; cependant, ils ne respectent pas / ne suivent pas la loi ou les normes éthiques à tout moment.	Par exemple, quelqu'un supprime un site frauduleux.
Chapeau noir	Ces personnes sont des criminels et cherchent souvent à nuire aux organisations ou à obtenir une certaine forme d'avantage financier au détriment des autres.	Par exemple, les auteurs de rançongiciels infectent les appareils avec du code malveillant et conservent les données contre une rançon.

Règles d'engagement ( RE)

Le ROE est un document qui est créé aux premières étapes d'un engagement de test d'intrusion. Ce document se compose de trois sections principales (expliquées dans le tableau ci-dessous), qui sont responsables en dernier ressort de décider de la manière dont la mission est menée. L'institut SANS a un excellent exemple de ce document que vous pouvez consulter en ligne ici .

Section	La description
Autorisation	Cette section du document autorise explicitement la réalisation de la mission. Cette autorisation est essentielle pour protéger juridiquement les individus et les organisations pour les activités qu'ils mènent.
Portée des tests	Cette section du document annotera les cibles spécifiques auxquelles l'engagement doit s'appliquer. Par exemple, le test d'intrusion peut ne s'appliquer qu'à certains serveurs ou applications, mais pas à l'ensemble du réseau.
Règles	La section des règles définira exactement les techniques autorisées lors de l'engagement. Par exemple, les règles peuvent stipuler spécifiquement que des techniques telles que les attaques de phishing sont interdites, mais les attaques MITM (Man-in-the-Middle) sont acceptables.

Méthodologies des tests d'intrusion

Les tests d'intrusion peuvent avoir une grande variété d'objectifs et de cibles dans leur portée. Pour cette raison, aucun test d'intrusion n'est identique, et il n'y a pas de cas unique quant à la façon dont un testeur d'intrusion devrait l'aborder.

Les étapes suivies par un testeur d'intrusion lors d'un engagement sont appelées la méthodologie. Une méthodologie pratique est une méthodologie intelligente, où les mesures prises sont pertinentes pour la situation actuelle. Par exemple, avoir une méthodologie que vous utiliseriez pour tester la sécurité d'une application Web n'est pas pratique lorsque vous devez tester la sécurité d'un réseau.

Avant de discuter de différentes méthodologies standard de l'industrie, nous devons noter que toutes ont un thème général des étapes suivantes :

Organiser	La description
La collecte d'informations	Cette étape implique de collecter autant d'informations accessibles au public sur une cible/organisation que possible, par exemple, OSINT et la recherche. **Remarque :** Cela n'implique pas l'analyse des systèmes.
Énumération/balayage	Cette étape implique la découverte des applications et des services exécutés sur les systèmes. Par exemple, trouver un serveur Web potentiellement vulnérable.
Exploitation	Cette étape consiste à exploiter les vulnérabilités découvertes sur un système ou une application. Cette étape peut impliquer l'utilisation d'exploits publics ou l'exploitation de la logique d'application.
Escalade des privilèges	Une fois que vous avez réussi à exploiter un système ou une application (connue sous le nom de foothold), cette étape est la tentative d'étendre votre accès à un système. Vous pouvez escalader horizontalement et verticalement, où horizontalement accède à un autre compte du même groupe d'autorisations (c'est-à-dire un autre utilisateur), alors que verticalement c'est celui d'un autre groupe d'autorisations (c'est-à-dire un administrateur).
Post-exploitation	Cette étape comporte quelques sous-étapes : **1.** Quels autres hébergeurs peuvent être ciblés (pivot) **2.** Quelles informations supplémentaires pouvons-nous recueillir auprès de l'hébergeur maintenant que nous sommes un utilisateur privilégié **3.** Couvrir vos traces **4.** Rapports

OSSTMM

Le manuel de méthodologie de test de sécurité Open Source fournit un cadre détaillé des stratégies de test pour les systèmes, les logiciels, les applications, les communications et l'aspect humain de la cybersécurité.

La méthodologie se concentre principalement sur la façon dont ces systèmes, applications communiquent, elle comprend donc une méthodologie pour :

1. **Télécommunications (téléphones, VoIP, etc.)**
2. Réseaux filaires
3. Communications sans fil

Avantages	Désavantages
Couvre en profondeur diverses stratégies de test.	Le cadre est difficile à comprendre, très détaillé et a tendance à utiliser des définitions uniques.
Comprend des stratégies de test pour des cibles spécifiques (c.-à-d. télécommunications et réseaux)	*Intentionnellement laissé en blanc.*
Le cadre est flexible en fonction des besoins de l'organisation.	*Intentionnellement laissé en blanc.*
Le cadre est destiné à établir une norme pour les systèmes et les applications, ce qui signifie qu'une méthodologie universelle peut être utilisée dans un scénario de test d'intrusion.	*Intentionnellement laissé en blanc.*

OWASP

Le framework « Open Web Application Security Project » est un framework piloté par la communauté et fréquemment mis à jour, utilisé uniquement pour tester la sécurité des applications et des services Web.

régulièrement rédige indiquant les dix principales vulnérabilités de sécurité qu'une application Web peut avoir, l'approche de test et la correction.

Avantages	Désavantages
Facile à saisir et à comprendre.	Le type de vulnérabilité d'une application Web peut ne pas être clair (elles peuvent souvent se chevaucher).
Maintenu activement et fréquemment mis à jour.	L'OWASP ne fait aucune suggestion concernant des cycles de vie de développement de logiciels spécifiques.
Il couvre toutes les étapes d'un engagement : des tests aux rapports et à la correction.	Le cadre ne détient aucune accréditation telle que CHECK.
Spécialisé dans les applications et services web.	*Intentionnellement laissé en blanc.*

NIST Cadre de cybersécurité

Le NIST Cybersecurity Framework est un cadre populaire utilisé pour améliorer les normes de cybersécurité d'une organisation et gérer le risque de cybermenaces. Ce cadre est un peu une mention honorable en raison de sa popularité et de ses détails.

Le cadre fournit des lignes directrices sur les contrôles de sécurité et des critères de réussite pour les organisations, des infrastructures critiques (centrales électriques, etc.) jusqu'au commercial. Il y a une section limitée sur une directive standard pour la méthodologie qu'un testeur d'intrusion devrait suivre.

Avantages	Désavantages
On NIST Framework sera utilisé par 50% des organisations américaines d'ici 2020.	Le NIST a de nombreuses itérations de cadres, il peut donc être difficile de décider lequel s'applique à votre organisation.
Le cadre est extrêmement détaillé dans l'établissement de normes pour aider les organisations à atténuer la menace posée par les cybermenaces.	Le NIST a des politiques d'audit faibles, ce qui rend difficile de déterminer comment une violation s'est produite.
Le cadre est très fréquemment mis à jour.	Le cadre ne prend pas en compte le cloud computing, qui devient rapidement de plus en plus populaire pour les organisations.
Le NIST fournit une accréditation aux organisations qui utilisent ce cadre.	*Intentionnellement laissé en blanc.*
Le NIST est conçu pour être mis en œuvre avec d'autres frameworks.	*Intentionnellement laissé en blanc.*

NCSC CAF

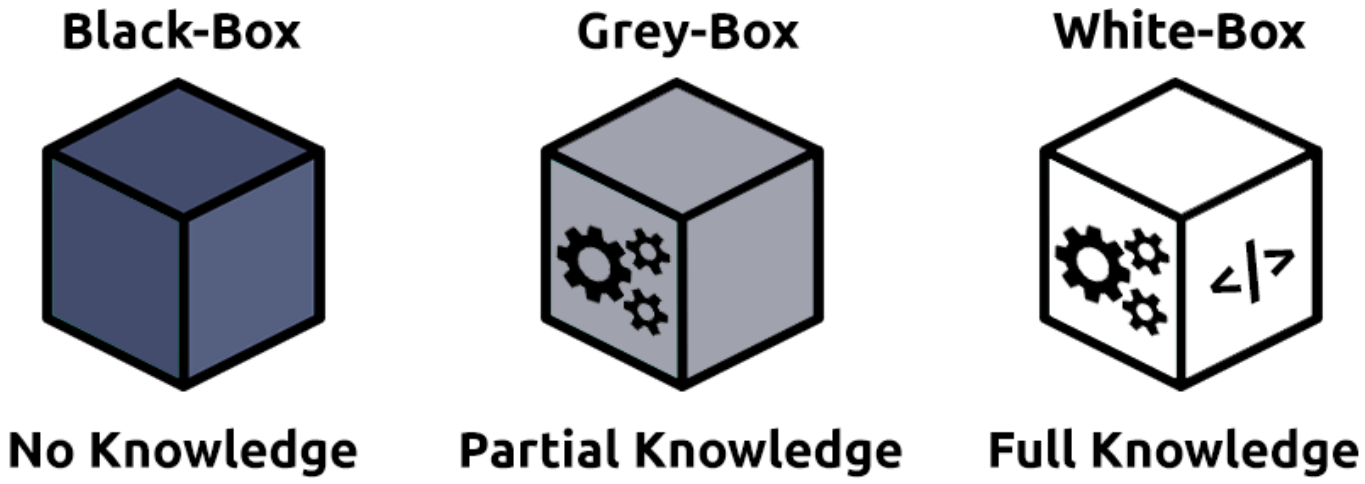
Le Cyber Assessment Framework (CAF) est un cadre étendu de quatorze principes utilisés pour évaluer le risque de diverses cybermenaces et les défenses d'une organisation contre celles-ci.

Le cadre s'applique aux organisations considérées comme exécutant des "services et activités d'une importance vitale" telles que les infrastructures critiques, les banques, etc. Le cadre se concentre principalement sur et évalue les sujets suivants :

- Sécurité des données
- Sécurité du système
- Identité et contrôle d'accès
- Élasticité
- Surveillance
- Planification de la réponse et du rétablissement

Avantages	Désavantages
Ce cadre est soutenu par une agence gouvernementale de cybersécurité.	Le cadre est encore nouveau dans l'industrie, ce qui signifie que les organisations n'ont pas eu beaucoup de temps pour apporter les modifications nécessaires pour s'y adapter.
Ce cadre fournit une accréditation.	Le cadre est basé sur des principes et des idées et n'est pas aussi direct que d'avoir des règles comme certains autres cadres.
Ce cadre couvre quatorze principes qui vont de la sécurité à la réponse.	Intentionnellement laissé en blanc.

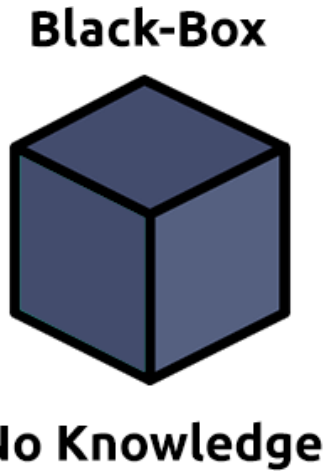
Boîte noire, boîte blanche, boîte grise Test d'intrusion



No Knowledge Partial Knowledge Full Knowledge

Il existe trois portées principales lors du test d'une application ou d'un service. Votre compréhension de votre cible déterminera le niveau de test que vous effectuerez dans votre mission de test d'intrusion. Dans cette tâche, nous couvrirons ces trois portées de test différentes.

Test de boîte noire



Ce processus de test est un processus de haut niveau dans lequel le testeur ne reçoit aucune information sur le fonctionnement interne de l'application ou du service.

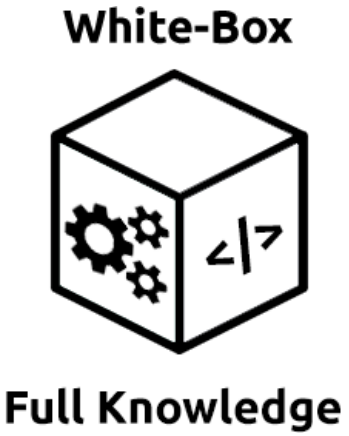
Le testeur agit comme un utilisateur régulier testant la fonctionnalité et l'interaction de l'application ou du logiciel. Ce test peut impliquer une interaction avec l'interface, c'est-à-dire des boutons, et un test pour voir si le résultat escompté est renvoyé. Aucune connaissance en programmation ou compréhension du programme n'est nécessaire pour ce type de test.
Les tests Black-Box augmentent considérablement le temps passé pendant la phase de collecte et d'énumération des informations pour comprendre la surface d'attaque de la cible.

Tests en boîte grise

Ce processus de test est le plus populaire pour des choses telles que les tests de pénétration. Il s'agit d'une combinaison de processus de test en boîte noire et en boîte blanche. Le testeur aura une **limitée** des composants internes de l'application ou du logiciel. Pourtant, il interagira avec l'application comme s'il s'agissait d'un scénario de boîte noire, puis utilisera leur connaissance de l'application pour essayer de résoudre les problèmes au fur et à mesure qu'ils les trouveront.

Avec les tests Grey-Box, les connaissances limitées fournies permettent de gagner du temps et sont souvent choisies pour des surfaces d'attaque extrêmement bien durcies.

Tests en boîte blanche



Ce processus de test est un processus de bas niveau généralement effectué par un développeur de logiciels qui connaît la programmation et la logique d'application. Le testeur testera les composants internes de l'application ou du logiciel et, par exemple, s'assurera que des fonctions spécifiques fonctionnent correctement et dans un délai raisonnable.

Le testeur aura **complété** de l'application et de son comportement attendu et prend beaucoup plus de temps que les tests en boîte noire. La connaissance complète d'un scénario de test White-Box fournit une approche de test qui garantit que toute la surface d'attaque peut être validée.
Répondre aux questions ci-dessous

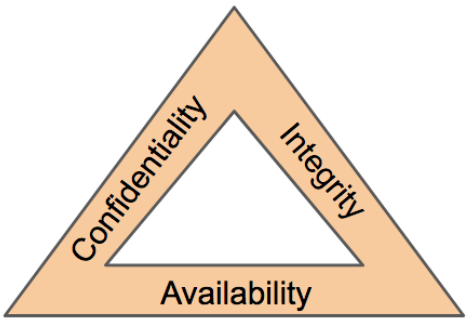
Principes de sécurité

La triade de la CIA

La triade CIA est un modèle de sécurité de l'information qui est utilisé en considération tout au long de la création d'une politique de sécurité. Ce modèle a une longue expérience, allant de son utilisation en 1998.

Cet historique est dû au fait que la sécurité des informations (sécurité de l'information) ne commence pas et/ou ne se termine pas avec la cybersécurité, mais s'applique plutôt à des scénarios tels que le classement, le stockage des enregistrements, etc.

Constitué de trois sections : **C**onfidentialité, **Intégrité** et. Disponibilité (CIA**)**, ce modèle est rapidement devenu un standard de l'industrie aujourd'hui Ce modèle devrait aider à déterminer la valeur des données auxquelles il s'applique et, à son tour, l'attention dont il a besoin de la part de l'entreprise.



La triade CIA est différente d'un modèle traditionnel où vous avez des sections individuelles ; il s'agit plutôt d'un cycle continu. Alors que les trois éléments de la triade de la CIA peuvent sans doute se chevaucher, si même un seul élément n'est pas satisfait, les deux autres sont rendus inutiles (similaire au triangle du feu). Si une politique de sécurité ne répond pas à ces trois sections, il s'agit rarement d'une politique de sécurité efficace.

Alors que les trois éléments de la triade CIA sont sans doute explicites, explorons-les et contextualisons-les dans la cybersécurité.

Confidentialité
Cet élément est la protection des données contre les accès non autorisés et les abus. Les organisations auront toujours une certaine forme de données sensibles stockées sur leurs systèmes. Assurer la confidentialité, c'est protéger ces données des tiers auxquels elles ne sont pas destinées.

Il existe de nombreux exemples concrets pour cela, par exemple, les dossiers des employés et les documents comptables seront considérés comme sensibles. La confidentialité sera assurée dans le sens où seuls les administrateurs RH auront accès aux dossiers des employés, où des vérifications et des contrôles d'accès stricts sont en place. Les documents comptables sont moins précieux (et donc moins sensibles), donc pas car des contrôles d'accès stricts seraient en place pour ces documents. Ou, par exemple, les gouvernements utilisant un système de classification de sensibilité (top-secret, classifié, non classifié)

Intégrité
L'élément d'intégrité de la triade de la CIA est la condition dans laquelle les informations sont maintenues exactes et cohérentes à moins que des modifications autorisées ne soient apportées. Il est possible que les informations changent en raison d'un accès et d'une utilisation imprudents, d'erreurs dans le système d'information ou d'un accès et d'une utilisation non autorisés. Dans la triade CIA, l'intégrité est maintenue lorsque les informations restent inchangées pendant le stockage, la transmission et l'utilisation n'impliquant pas de modification des informations. Des mesures doivent être prises pour s'assurer que les données ne peuvent pas être modifiées par des personnes non autorisées (par exemple, en cas de violation de la confidentialité).

De nombreuses défenses pour assurer l'intégrité peuvent être mises en place. Un contrôle d'accès et une authentification rigoureuse peuvent aider à empêcher les utilisateurs autorisés d'effectuer des modifications non autorisées. Les vérifications de hachage et les signatures numériques peuvent aider à garantir que les transactions sont authentiques et que les fichiers n'ont pas été modifiés ou corrompus.

Disponibilité
Pour que les données soient utiles, elles doivent être disponibles et accessibles par l'utilisateur.

La principale préoccupation de la triade CIA est que les informations soient disponibles lorsque les utilisateurs autorisés doivent y accéder.

La disponibilité est très souvent un critère clé pour une organisation. Par exemple, avoir une disponibilité de 99,99 % sur leurs sites Web ou leurs systèmes (cela est défini dans les accords de niveau de service). Lorsqu'un système n'est pas disponible, il en résulte souvent des dommages à la réputation d'une organisation et une perte de finances. La disponibilité est obtenue grâce à une combinaison de nombreux éléments, notamment :

- Avoir du matériel fiable et bien testé pour leurs serveurs de technologie de l'information (c'est-à-dire des serveurs réputés)
- Avoir une technologie et des services redondants en cas de panne du primaire
- Mettre en œuvre des protocoles de sécurité bien rodés pour protéger la technologie et les services contre les attaques

Principes des privilèges

Il est essentiel d'administrer et de définir correctement les différents niveaux d'accès à un système informatique dont les individus ont besoin.

Les niveaux d'accès accordés aux individus sont déterminés en fonction de deux facteurs principaux :

- Le rôle/la fonction de l'individu au sein de l'organisation
- La sensibilité des informations stockées sur le système

Deux concepts clés sont utilisés pour attribuer et gérer les droits d'accès des individus, deux concepts clés sont utilisés : Privileged Identity Management (PIM) et Privileged Access Management (ou PAM en abrégé).

Au départ, ces deux concepts peuvent sembler se chevaucher ; cependant, ils sont différents les uns des autres. PIM est utilisé pour traduire le rôle d'un utilisateur au sein d'une organisation en un rôle d'accès sur un système. Alors que PAM est la gestion des privilèges du rôle d'accès d'un système, entre autres choses.

Ce qui est essentiel lorsqu'il est question de privilèges et de contrôles d'accès, c'est le principe du moindre privilège. Simplement, les utilisateurs doivent recevoir le minimum de privilèges, et uniquement ceux qui leur sont absolument nécessaires pour accomplir leurs tâches. Les autres personnes devraient pouvoir faire confiance à ce à quoi les gens écrivent.

Comme nous l'avons mentionné précédemment, PAM intègre plus que l'attribution d'accès. Cela englobe également l'application de politiques de sécurité telles que la gestion des mots de passe, les politiques d'audit et la réduction de la surface d'attaque à laquelle un système est confronté.

Modèles de sécurité (suite)

Avant de discuter plus en détail des modèles de sécurité, rappelons les trois éléments de la triade CIA : confidentialité, intégrité et disponibilité. Nous avons décrit précédemment ce que sont ces éléments et leur importance. Cependant, il existe un moyen formel d'y parvenir.

Selon un modèle de sécurité, tout système ou élément technologique stockant des informations est appelé un système d'information, c'est ainsi que nous référencerons les systèmes et les appareils dans cette tâche.

Explorons quelques modèles de sécurité populaires et efficaces utilisés pour réaliser les trois éléments de la triade CIA.

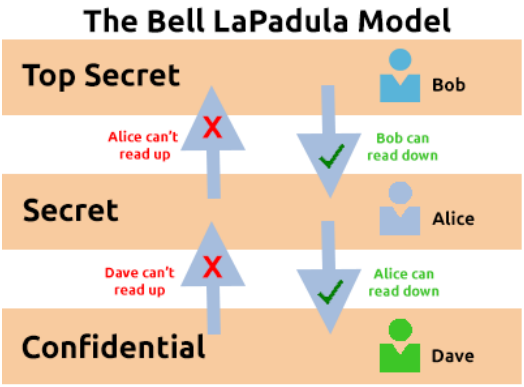
Bell-La Padula modèle

Le modèle Bell-La Padula est utilisé pour assurer la confidentialité. Ce modèle repose sur quelques hypothèses, telles que la structure hiérarchique d'une organisation dans laquelle il est utilisé, où les responsabilités/rôles de chacun sont bien définis.

Le modèle fonctionne en accordant l'accès à des éléments de données (appelés objets) sur une base strictement nécessaire. Ce modèle utilise la règle "pas d'écriture, pas de lecture".

Avantages	Désavantages
Les politiques de ce modèle peuvent être répliquées dans des hiérarchies d'organisations réelles (et vice versa)	Même si un utilisateur n'a pas accès à un objet, il connaîtra son existence -- il n'est donc pas confidentiel à cet égard.
Simple à mettre en œuvre et à comprendre, et a fait ses preuves.	Le modèle repose sur une grande confiance au sein de l'organisation.

Le modèle Bell LaPadula est populaire au sein d'organisations telles que gouvernementales et militaires. En effet, les membres des organisations sont présumés avoir déjà suivi un processus appelé vérification. La vérification est un processus de sélection où les antécédents des candidats sont examinés pour établir le risque qu'ils représentent pour l'organisation. Par conséquent, les candidats qui sont examinés avec succès sont supposés être dignes de confiance - c'est là que ce modèle s'intègre.



Modèle Biba

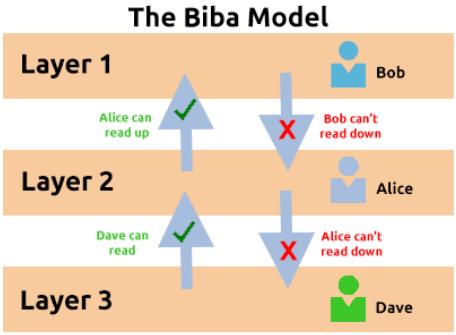
Le modèle Biba est sans doute l'équivalent du modèle Bell-La Padula mais pour l'intégrité de la triade CIA.

Ce modèle applique la règle aux objets (données) et aux sujets (utilisateurs) qui peuvent être résumés par "pas d'écriture, pas de lecture". Cette règle signifie que les sujets **peuvent** créer ou écrire du contenu sur des objets à leur niveau ou en dessous, mais **ne peuvent** lire que le contenu des objets au-dessus du niveau du sujet.

Comparons quelques avantages et inconvénients de ce modèle dans le tableau ci-dessous :

Avantages	Désavantages
Ce modèle est simple à mettre en œuvre.	Il y aura plusieurs niveaux d'accès et d'objets. Les choses peuvent être facilement négligées lors de l'application des contrôles de sécurité.
Résout les limites du modèle Bell-La Padula en traitant à la fois la confidentialité et l'intégrité des données.	Entraîne souvent des retards au sein d'une entreprise. Par exemple, un médecin ne pourrait pas lire les notes prises par une infirmière dans un hôpital avec ce modèle.

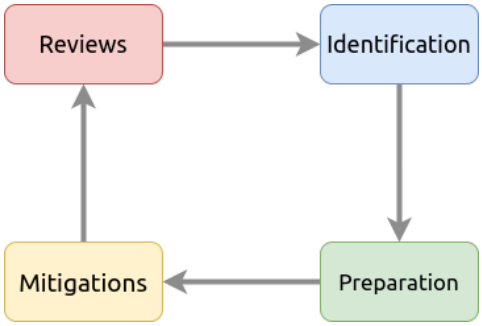
Le modèle Biba est utilisé dans des organisations ou des situations où l'intégrité est plus importante que la confidentialité. Par exemple, dans le développement de logiciels, les développeurs peuvent n'avoir accès qu'au code nécessaire à leur travail. Ils peuvent ne pas avoir besoin d'accéder à des éléments d'information critiques tels que des bases de données, etc.



Modélisation des menaces et réponse aux incidents

La modélisation des menaces est le processus d'examen, d'amélioration et de test des protocoles de sécurité en place dans l'infrastructure et les services de technologie de l'information d'une organisation.

Une étape critique du processus de modélisation des menaces consiste à identifier les menaces probables auxquelles une application ou un système peut être confronté, les vulnérabilités auxquelles un système ou une application peut être vulnérable.



Le processus de modélisation des menaces est très similaire à une évaluation des risques effectuée sur les lieux de travail pour les employés et les clients. Les principes reviennent tous à :

- Préparation
- Identification
- Atténuations
- Examen

Il s'agit cependant d'un processus complexe qui nécessite un examen et une discussion constants avec une équipe dédiée. Un modèle de menace efficace comprend :

- Renseignements sur les menaces
- Identification des actifs
- Capacités d'atténuation
- L'évaluation des risques

Pour aider à cela, il existe des frameworks tels que **STRIDE** (**S** poofing identity, **Tampering** with data, **R** epudiation Menaces, **I** , **D** enial of Service and **rocess** Elevation of Privilèges) et **PASTA** (**P** for **A** ttack **S** imulation and **T** hreat **A** nalysis) infosec n'a jamais été aussi bon !. Détaillons STRIDE ci-dessous. STRIDE, rédigé par deux chercheurs en sécurité de Microsoft en 1999, est toujours d'actualité aujourd'hui. STRIDE comprend six grands principes, que j'ai détaillés dans le tableau ci-dessous :

Principe	La description
Usurpation	Ce principe vous oblige à authentifier les requêtes et les utilisateurs accédant à un système. L'usurpation d'identité implique qu'une partie malveillante s'identifie à tort comme une autre. Les clés d'accès (telles que les clés API) ou les signatures via le chiffrement permettent de remédier à cette menace.

Falsification	En fournissant des mesures anti-falsification à un système ou à une application, vous contribuez à assurer l'intégrité des données. Les données consultées doivent rester intégrales et exactes. Par exemple, les magasins utilisent des sceaux sur les produits alimentaires.
Répudiation	Ce principe dicte l'utilisation de services tels que la journalisation de l'activité d'un système ou d'une application à suivre.
Divulgation d'information	Les applications ou les services qui gèrent les informations de plusieurs utilisateurs doivent être correctement configurés pour afficher uniquement les informations pertinentes pour le propriétaire.
Déni de service	Les applications et les services utilisent les ressources système, ces deux choses doivent avoir des mesures en place afin que l'abus de l'application/du service n'entraîne pas la panne de l'ensemble du système.
Élévation de privilège	Il s'agit du pire scénario pour une application ou un service. Cela signifie qu'un utilisateur a pu faire passer son autorisation à celle d'un niveau supérieur, c'est-à-dire un administrateur. Ce scénario conduit souvent à une exploitation plus poussée ou à la divulgation d'informations.

Une violation de la sécurité est connue sous le nom d'incident. Et malgré tous les modèles de menaces rigoureux et les conceptions de systèmes sécurisés, des incidents se produisent. Les mesures prises pour résoudre et remédier à la menace sont connues sous le nom de réponse aux incidents (IR) et constituent tout un cheminement de carrière dans la cybersécurité.

Les incidents sont classés selon une cote d'urgence et d'impact. L'urgence sera déterminée par le type d'attaque rencontrée, où l'impact sera déterminé par le système affecté et quel impact cela a sur les opérations commerciales.

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

Un incident est traité par une équipe de réponse aux incidents de **est** sécurité) informatique **(** CSIRT **qui** un **d'** groupe **préétabli** employés ayant des connaissances techniques sur les systèmes et/ou l'incident en cours. Pour résoudre un incident avec succès, ces étapes sont souvent appelées les six phases de réponse aux incidents qui ont lieu, répertoriées dans le tableau ci-dessous :

Action	La description
Préparation	Avons-nous les ressources et les plans en place pour faire face à l'incident de sécurité ?
Identification	La menace et l'auteur de la menace ont-ils été correctement identifiés afin que nous puissions y répondre ?
Endiguement	La menace/l'incident de sécurité peut-il être contenu pour empêcher d'autres systèmes ou utilisateurs d'être impactés ?
Éradication	Supprimez la menace active.
Récupération	Effectuez un examen complet des systèmes concernés pour revenir aux opérations habituelles.
Leçons apprises	Que peut-on retenir de l'incident ? C'est-à-dire que si cela était dû à un e-mail de phishing, les employés devraient être mieux formés pour détecter les e-mails de phishing.