ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Identification des menaces de sécurité réseau

www.ofppt.info

OFPPT

DIRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

SECTEUR NTIC

Sommaire

h

1. Présentation des menaces à la sécurité

1.1. Introduction

Une menace décrit un danger ou une vulnérabilité. Les menaces peuvent Survenir à partir de sources diverses, par exemple des attaques ou une application mal configurée.

1.2. Pourquoi des attaques de réseaux ont-elles lieu

Des intrus tentent de compromettre la sécurité des réseaux et des applications pour diverses raisons :

- **Vengeance**. Un intrus peut estimer avoir subi un affront de la part d'une organisation et souhaite s'en prendre à elle. Il arrive que d'anciens employés attaquent leurs anciens employeurs par vengeance. Ce type d'intrus est particulièrement dangereux par sa connaissance intime du réseau et sa motivation personnelle.

- **Espionnage**. Un intrus peut espionner une organisation ou un gouvernement afin d'obtenir des secrets. Ce type d'intrus est souvent motivé par le patriotisme ou l'appât du gain.

- **Publicité**. Un intrus peut attaquer un réseau ou une application pour se faire connaître auprès du public ou pour se faire de la publicité pour ses propres services. Les intrus à la recherche de publicité font souvent état de leurs attaques.

- **Satisfaction personnelle**. Un intrus peut attaquer des réseaux comme passetemps, pour le défi que cela représente ou pour son autosatisfaction. Ce type d'intrus est dangereux par les efforts qu'ils déploie à attaquer n'importe quel réseau.

- **Terrorisme**. Un intrus peut attaquer un réseau dans le cadre d'une opération de terrorisme d'état ou émanant d'un groupe. Il s'agit des types d'intrus les plus graves car il se peut que des vies humaines soient alors en danger.

1.3. Qui attaque des réseaux ?

Les intrus, quelles que soient leurs aptitudes et leurs motivations, sont dangereux pour la sécurité d'un réseau à titres divers :

- **Novice**. La plupart des intrus ne possèdent que des connaissances
- informatiques rudimentaires, mais ils sont néanmoins dangereux parce qu'il est fréquent qu'ils ne réalisent pas totalement les conséquences de leurs actions.

- **Intermédiaire**. Les intrus possédant des connaissances intermédiaires tentent souvent de s'attirer du respect de la part des communautés de hackers. Ils attaquent généralement des cibles importantes ou créent des outils automatisés permettant à des tiers d'attaquer des réseaux.

- **Avancés**. Les intrus très compétents représentent un sérieux défi pour la sécurité d'un réseau parce que leurs méthodes d'attaque peuvent ne pas se cantonner à la technologie, mais inclure une intrusion physique et la manipulation des structures sociales, ou encore tromper un utilisateur ou un administrateur afin d'obtenir des informations. Bien qu'il existe relativement peu d'intrus hautement qualifiés, leurs talents et leur expérience font d'eux les intrus les plus dangereux pour un réseau.

1.4. Types courants de vulnérabilité des réseaux

Vulnérabilité	Exemples
Mots de passe faibles	• Les employés utilisent des mots de passe vierges ou les mots de passe définis par défaut • Le mot de passe est prévisible
Logiciels sans correctif	• Les Service Packs ne sont pas gérés • Les correctifs de sécurité ne sont pas appliqués
Matériel et logiciel mal configurés	• Les utilisateurs disposent de trop de privilèges • Les applications sont exécutées sous le compte système local
Piratage informatique	• L'administrateur de l'assistance technique réinitialise un mot de passe sans vérifier l'identité de la personne qui émet la demande
Sécurité faible des connexions Internet	• Les services et ports non utilisés ne sont pas sécurisés • Les pare-feu et routeurs sont utilisés de manière incorrecte
Transfert non crypté des données	• Les paquets d'authentification sont envoyés en texte clair • Les données importantes sont envoyées sur Internet en texte clair

La plupart des attaques réussies sur les réseaux parviennent à leur fin en

exploitant des vulnérabilités ou des faiblesses bien connues. Assurez-vous de former les administrateurs à reconnaître ces vulnérabilités et à se familiariser avec les nouvelles failles de sécurité que l'on découvre.

1.5. Comment se produisent les attaques sur les réseaux

Les attaques de réseaux reproduisent souvent le même schéma. Vous devez concevoir des méthodes pour détecter, réagir ou empêcher les attaques durant chacune des étapes suivantes :

1. **Inventaire**. À ce stade, l'intrus étudie l'organisation cible. Il peut obtenir toutes les informations publiques concernant une organisation et ses employés et analyser tous les ports sur tous les ordinateurs et périphériques accessibles à partir d'Internet.

2. **Pénétration**. Après que l'intrus ait localisé des vulnérabilités potentielles, il va s'efforcer de s'infiltrer par l'une d'entre elles. Par exemple, l'intrus exploite un serveur Web ne possédant pas la mise à jour de sécurité la plus récente.

3. **Élévation de privilège**. Après que l'intrus ait pénétré le réseau, il s'efforce d'obtenir les autorisations de niveau administrateur ou système.
Par exemple, alors qu'il exploite le serveur Web, il parvient à prendre le contrôle d'un processus s'exécutant sous le contexte de sécurité LocalSystem et utilise ce processus pour créer un compte administrateur. Souvent, une sécurité insuffisante liée à l'utilisation de paramètres par défaut permet à un intrus d'obtenir l'accès à un réseau sans trop d'efforts.

4. **Exploitation**. Après que l'intrus ait obtenu les autorisations nécessaires, il exploite la méthode qui lui a permis de pénétrer dans le réseau par effraction. Par exemple, l'intrus choisit de modifier le site Web public de l'organisation.

5. **Élimination** de toute trace. La dernière étape d'une attaque consiste pour un intrus à masquer ses actions afin de ne pas être détecté ou de ne pas faire l'objet de poursuites. Par exemple, un intrus efface les entrées le concernant dans les fichiers d'audit du système.

2. Prédiction des menaces à la sécurité

2.1. Introduction

L'aptitude à prédire des menaces vous aidera à affecter des priorités aux dépenses liées aux ressources de sécurité destinées à protéger votre réseau. Les menaces changent chaque jour, en fonction des modifications technologiques. L'utilisation d'une technique connue sous le nom de modélisation des menaces vous aidera à prévoir les points où des attaques peuvent survenir sur votre réseau.

2.2. Modèle de menace

Un modèle de menace est une approche structurée qui vous aide à prédire les menaces potentielles pesant sur la sécurité des informations. La menace potentielle que vous découvrez lorsque vous effectuez une modélisation des menaces vous permet de créer un plan précis de gestion des risques. La prédiction des menaces vous permet de réduire votre risque de manière proactive.
Le modèle STRIDE est une manière simple de classer les menaces en fonction de leurs caractéristiques. Le modèle STRIDE comporte six catégories de menaces.

Types de menaces	Exemples
Spoofing (usurpation)	• Crée des messages électroniques • Relance les paquets d'authentification
Tampering (falsification)	• Modifie les données au cours de leur transmission • Modifie les données dans les fichiers
Repudiation (répudiation)	• Supprime un fichier important et le nie • Achète un produit, puis le nie
Information disclosure (divulgation d'informations)	• Divulgation d'informations dans les messages d'erreur • Divulgation de code sur les sites Web
Denial of service (refus de service)	• Submerge le réseau de paquets SYN • Submerge le réseau de paquets ICMP créés
Élévation de privilège	• Exploite la saturation au niveau de la mémoire tampon pour obtenir les privilèges système • Obtient les privilèges administrateur de manière illégale

.

2.3. Étapes requises pour la prédiction de menaces à l'aide d'un modèle de menace

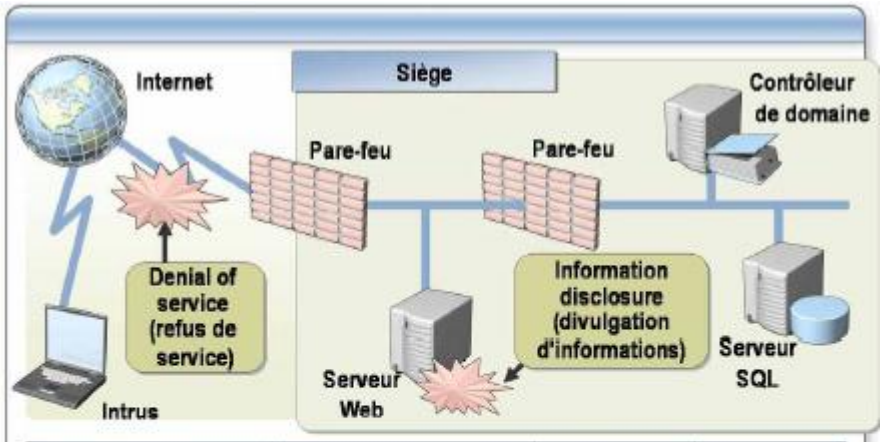
Pour utiliser un modèle de menace, tel que STRIDE, procédez comme suit :

1. ***Définissez l'étendue***. Décidez quels matériels et quels logiciels vous allez évaluer au cours de l'exercice de modélisation des menaces. En définissant les matériels et les logiciels, vous pouvez vous concentrer exclusivement sur l'objet de la modélisation des menaces, par exemple un serveur Web ou une filiale, plutôt que le réseau tout entier.

2. ***Créez une équipe***. L'équipe doit inclure diverses expériences et compétences techniques. L'idéal serait que chaque membre de l'équipe puisse se représenter l'objet de l'exercice de modélisation des menaces à partir de nombreuses perspectives, y compris celles qui peuvent sembler bizarres ou être illégales. Pour préserver l'objectivité, choisissez des membres de l'équipe ayant peu à faire avec l'objet de la modélisation des menaces.

3. ***Prédisez les menaces***. Équipez-vous de tableaux blancs et à feuilles mobiles ainsi que de documentations pertinentes pour discuter des possibles manières permettant d'attaquer l'objet. Prévoyez plusieurs sessions de courte durée afin que les membres de l'équipe aient le temps de réfléchir à l'objet. Demandez à quelqu'un de documenter ce que l'équipe aura déterminé.

2.4. Comment créer un modèle de menace portant sur une infrastructure

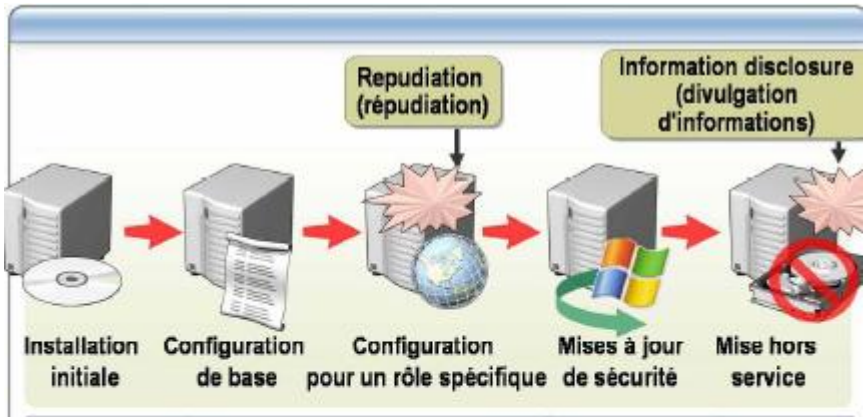


Type	Menace	Probabilité	Impact
Denial of service (refus de service)	Une attaque automatisée stoppe le trafic légal des données	Élevée	Moyen - élevé
Information disclosure (divulgation d'informations)	Un compte SA est utilisé dans les chaînes de requête SQL	Moyenne	Critique

Une approche de la modélisation des menaces consiste à appliquer le modèle STRIDE à une section bien définie de l'infrastructure du réseau. Par exemple, vous pouvez souhaiter isoler un serveur Web pour une modélisation des menaces.
Lorsque vous effectuez une modélisation des menaces sur des infrastructures, vérifiez que vous disposez de toute la documentation pertinente, y compris :

- Les diagrammes de réseau.
- Les configurations matérielles et logicielles.
- Les diagrammes des flux de données.
- Le code source personnalisé.

2.5. Comment créer un modèle de menace portant sur le cycle de vie



Type	Menace	Probabilité	Impact
Repudiation (répudiation)	Audit non activé au cours de la configuration du serveur Web	Moyenne	Moyen - élevé
Information disclosure (divulgation d'informations)	Les données restent sur le disque dur	Moyenne	Élevé

Une autre approche de la modélisation des menaces consiste à appliquer le modèle STRIDE au cycle de vie d'un périphérique ou d'une application. Par exemple, vous pouvez prédire les menaces pesant sur les ordinateurs déployés sur votre réseau. Comme la diapositive le montre, la vulnérabilité d'un ordinateur à différentes menaces dépend de l'étape de son cycle de vie.

Item a
Item b

Mettre l’accent sur un point particulier

Note d’attention particulière.

Pour approfondir le sujet….

Proposition de références utiles permettant d'approfondir le thème abordé

Sources de référence

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support