Travaux pratiques 1.4.5 Identification des vulnérabilités du réseau

Objectifs

- Utiliser le site SANS pour identifier rapidement les menaces de sécurité Internet
- Expliquer la façon dont les menaces sont organisées
- Répertorier plusieurs vulnérabilités de sécurité récentes
- Utiliser les liens SANS pour accéder à d'autres informations relatives à la sécurité

Objectifs de l'examen CCNA 640-802

Ces travaux pratiques font appel à des compétences qui se rapportent aux objectifs d'examen CCNA suivants :

- Décrire les pratiques de sécurité recommandées, y compris les phases initiales de sécurisation des périphériques réseau
- Décrire les menaces actuelles grandissantes auxquelles est confrontée la sécurité des réseaux et expliquer le besoin d'implémentation d'une politique complète de sécurité afin d'atténuer ces menaces
- Expliquer les méthodes générales de réduction des menaces de sécurité courantes auxquelles les périphériques, hôtes et applications réseau sont confrontés
- Décrire les fonctions des appareils et des applications de sécurité courants

Résultats attendus et critères de réussite

Avant de commencer ces travaux pratiques, lisez les tâches que vous devez effectuer. Selon vous, quel sera le résultat de l'exécution de ces tâches ?

_____

_____

_____

En quoi est-il utile d'avoir une compréhension des vulnérabilités du réseau en administration réseau ?

_____

_____

_____

Comment l'administrateur réseau maintient-il la sécurité du réseau ?

_____

_____

_____

Contexte / Préparation

SANS est l'un des sites les plus populaires et reconnus qui traitent de la lutte contre les menaces envers les ordinateurs et la sécurité de réseau. Il signifie SysAdmin, Audit, Network, Security (administrateur système, audit, réseau, sécurité). SANS comporte plusieurs composants qui ont tous une grande contribution à apporter à la sécurité de l'information. Pour plus de renseignements sur SANS, consultez http://www.sans.org/ et sélectionnez les éléments du menu **Resources**.

Comment un administrateur de sécurité d'entreprise peut-il rapidement identifier les menaces de sécurité ? En collaboration avec le FBI, SANS a compilé une liste des **20 cibles d'attaques de sécurité Internet les plus courantes** sur http://www.sans.org/top20/. La liste est régulièrement mise à jour dans les catégories suivantes :

- Systèmes d'exploitation : Windows, Unix/Linux, MAC
- Applications multiplateformes : comprennent le Web, les bases de données, le Peer to peer, la messagerie instantanée, les lecteurs multimédia, les serveurs DNS, les logiciels de sauvegarde et les serveurs d'administration
- Périphériques réseau : les périphériques d'infrastructure du réseau (routeurs, commutateurs etc.), les périphériques VoIP
- Politique et personnel de sécurité : politiques de sécurité, comportement du personnel et problèmes relatifs au personnel
- Section spéciale : stratégies de prévention et autres questions de sécurité

Dans ces travaux pratiques, il vous sera présenté des problèmes de sécurité et des vulnérabilités relatifs à l'ordinateur. Le site SANS est utilisé en tant qu'outil d'identification et de compréhension des vulnérabilités aux menaces ainsi que de lutte contre ces vulnérabilités.

Le temps pour effectuer ces travaux pratiques est estimé à une heure.

Étape 1 : ouverture de la liste SANS des 20 cibles les plus courantes

Au moyen d'un navigateur Web, rendez-vous à l'adresse http://www.sans.org/. Dans le menu **resources**, choisissez **top 20 list**.

La liste des **20 cibles d'attaques de sécurité Internet les plus courantes** est organisée par catégorie. Une lettre d'identification indique le type de la catégorie et leurs sujets sont numérotés. Ceux concernant les routeurs et les commutateurs se trouvent dans la catégorie **Network Devices , N**. Deux sujets principaux y sont présents (liens hypertexte) :

N1. VoIP Servers and Phones

N2. Network and Other Devices Common Configuration Weaknesses

Étape 2 : consultation des faiblesses courantes de configuration

a. Cliquez sur le lien hypertexte **N2. Network and Other Devices Common Configuration Weaknesses**.

b. Énumérez les quatre titres dans ce sujet.

_____

_____

_____

_____

Étape 3 : consultation des problèmes fréquents de configuration par défaut

Consultez le contenu de **N2.2 Common Default Configuration Issues**. À titre d'exemple, **N.2.2.2** contenait en janvier 2007 des informations sur les menaces associées aux comptes et valeurs par défaut. Une recherche Google « wireless router passwords » produit comme résultat des liens vers plusieurs sites publiant une liste des noms de comptes et des mots de passe administrateur par défaut pour les routeurs sans fil. Si les mots de passe par défaut ne sont pas changés sur ces appareils, cela peut entraîner la compromission de la sécurité et une vulnérabilité aux attaques.

Étape 4 : prise en note des références CVE

La dernière ligne située dans plusieurs sujets fait référence à CVE ou Common Vulnerability Exposure (Exposition aux vulnérabilités fréquentes). Le nom CVE est lié à la base de données nationale des vulnérabilités (NVD - National Vulnerability Database) du National Institute of Standards and Technology (NIST) sponsorisé par la division de la cyber-sécurité nationale du ministère américain de la sécurité nationale (DHS - United States Department of Homeland Security) et US-CERT. Cette base de données contient des informations sur la vulnérabilité.

Étape 5 : explorer un sujet et son lien hypertexte CVE associé

Le reste de ces travaux pratiques vous guident dans l'exploration d'une vulnérabilité et de sa solution.

Choisissez un sujet, puis cliquez sur le lien hypertexte CVE qui lui est associé. Le lien devrait ouvrir une nouvelle fenêtre de navigateur à la page http://nvd.nist.gov/ qui affiche le résumé de la vulnérabilité CVE.

REMARQUE : en raison de l'évolution de la liste CVE, la liste actuelle peut ne pas contenir les mêmes vulnérabilités que celles qui y figuraient en janvier 2007.

Étape 6 : relevé des informations de vulnérabilité

Remplissez les informations relatives à la vulnérabilité.

Date de version d'origine : _____

Dernière révision : _____

Source : _____

Vue d'ensemble : _____

_____

_____

_____

Étape 7 : relevé de l'impact de la vulnérabilité

Dans **Impact** figurent plusieurs valeurs. La sévérité CVSS (Common Vulnerability Scoring System) est affichée et contient une valeur comprise entre 1 et 10.

Remplissez les informations relatives à l'impact de la vulnérabilité.

Sévérité CVSS : _____

Complexité de l'accès : _____

Authentification : _____

Type d'impact : _____

Étape 8 : relevé de la solution

La section **References to Advisories, Solutions, and Tools** contient des liens vers des informations sur la vulnérabilité et ses solutions possibles.

Au moyen des liens hypertexte, écrivez une brève description de la solution trouvée sur ces pages.

_____

_____

_____

_____

_____

_____

_____

_____

Étape 9 : remarques générales

Le nombre des vulnérabilités des ordinateurs, réseaux et données ne cesse d'augmenter. De nombreux gouvernements ont consacré d'importantes ressources à la coordination et à la diffusion des informations sur les vulnérabilités de sécurité et les solutions possibles. La responsabilité de mise en œuvre de la solution revient encore à l'utilisateur final. Réfléchissez aux moyens par lesquels les utilisateurs peuvent faciliter le renforcement de la sécurité. Notez certaines habitudes qui créent des risques de sécurité.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Confirmation

Tentez de trouver un organisme prêt à rencontrer les participants afin d'expliquer la façon dont il effectue le suivi des vulnérabilités et applique les solutions. Un tel organisme peut être difficile à trouver pour des raisons de sécurité, mais cela sera avantageux pour les participants qui apprendront comment se déroule la réduction des vulnérabilités sur le terrain. Cela permettra également aux représentants de l'organisme de rencontrer les participants et de faire passer des entretiens informels de stagiaires.