Exercice 1.4.5 : Identification des principales failles de sécurité

Objectifs pédagogiques

À la fin de cet exercice, vous saurez :

- Utiliser le site SANS pour identifier rapidement les menaces de sécurités présentes sur Internet
- Expliquer la façon dont s'organisent les menaces
- Répertorier plusieurs failles de sécurité récentes
- Utiliser les liens SANS pour accéder à d'autres informations de sécurité

Contexte

Le site SANS est l'un des sites les plus populaires et efficaces en matière de défense contre les menaces de sécurité informatiques et réseau. SANS fait référence à SysAdmin, Audit, Network, Security (Administration système, audit, réseau, sécurité). SANS contient plusieurs composants, chacun contribuant de façon significative à la sécurité des informations. Pour plus d'informations sur le site SANS, accédez à l'URL http://www.sans.org/, puis sélectionnez des éléments dans le menu Resources.

Comment un administrateur de sécurité d'entreprise peut-il identifier rapidement les menaces de sécurité ? SANS et le FBI ont compilé la liste des 20 principales cibles d'attaque de sécurité Internet à l'adresse suivante : http://www.sans.org/top20/. La liste est régulièrement mise à jour avec des informations organisées en fonction des éléments suivants :

- systèmes d'exploitation : Windows, Unix/Linux, MAC ;
- applications : inter-plateformes, y compris Web, base de données, peer to peer, messagerie instantanée, lecteurs multimédias, serveurs DNS, logiciels de sauvegarde et serveurs de gestion ;
- périphériques réseau : périphériques d'infrastructure réseau (routeurs, commutateurs, etc.), périphériques VoIP ;
- éléments humains : règles de sécurité, comportement humain, problèmes personnels ;
- section spéciale : problèmes de sécurité étrangers aux catégories ci-dessus.

Scénario

Ces travaux pratiques vont permettre aux participants d'aborder les failles de sécurité informatiques. Le site Web SANS sera utilisé comme outil d'identification, de compréhension et de défense contre les menaces.

Ces travaux pratiques doivent être réalisés en dehors des travaux pratiques de Cisco, à partir d'un ordinateur doté d'un accès à Internet.

Cette session de travaux pratiques prend environ une heure.

Tâche 1 : localisation des ressources SANS

Étape 1 : ouverture de la liste SANS Top 20 List

À partir d'un navigateur Web, accédez à l'URL http://www.sans.org. Dans le menu **resources**, sélectionnez **top 20 list**, comme illustré dans la figure 1.

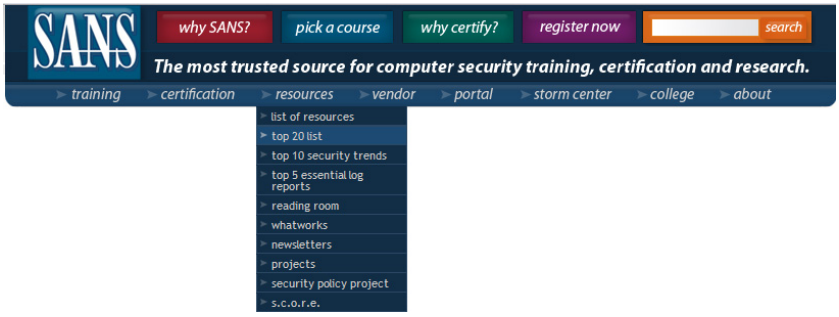

Figure 1. Menu SANS

La liste SANS Top-20 Internet Security Attack Targets est organisée par catégorie. Une lettre d'identification indique le type de catégorie. Les nombres permettent d'effectuer la distinction entre les différentes rubriques d'une même catégorie. Ces rubriques changent tous les ans en raison notamment de l'évolution rapide des technologies. Pour les besoins de cet exercice, accédez à l'URL http://www.sans.org/top20/2006/?portal=8cd2978e94c0c1ae18da87e90a085409.

Les rubriques Router et Switch appartiennent à la même catégorie : Network Devices, **N**. Il existe deux rubriques principales :

N1. VoIP Servers and Phones
N2. Network and Other Devices Common Configuration Weaknesses

Étape 2 : Cliquez sur N2. Network and Other Devices Common Configuration Weaknesses pour accéder à cette rubrique.

Tâche 2 : examen des ressources SANS

Étape 1 : examen du contenu de N2.2 Common Default Configuration Issues

Par exemple, N.2.2.2 (en janvier 2007) contient des informations sur les menaces associées aux comptes et aux valeurs par défaut. Une recherche dans Google sur « wireless router passwords » retourne des liens vers plusieurs sites qui publient une liste de mots de passe et de noms de comptes administrateur de routeurs sans fil. En l'absence de modification de ces mots de passe, les périphériques peuvent être exposés aux attaques.

Étape 2 : note des références CVE

La dernière ligne située sous les rubriques fait référence à l'exposition aux failles standard (CVE). Ce nom est lié à la National Vulnerability Database (NVD) du National Institute of Standards and Technology (NIST), sponsorisé par le Department of Homeland Security (DSH) National Cyber Security Division et l'US-CERT, qui contient des informations sur les failles.

Tâche 3 : collecte des données

Le reste des travaux pratiques est consacré à un exercice de recherche et de résolution de failles.

Étape 1 : choix d'un domaine à examiner, puis clic sur un exemple de lien hypertexte CVE

Remarque : en raison de la constante évolution de la liste CVE, la liste actuelle peut ne pas contenir les mêmes failles que celles observées en janvier 2007.

Le lien doit ouvrir un nouveau navigateur Web connecté à http://nvd.nist.gov/ et à la page de résumé des failles de la liste CVE.

Étape 2 : renseignement des informations sur la faille

Date de version d'origine : _____

Dernière révision : _____

Source : _____

Présentation générale :

_____

_____

_____

_____

_____

Plusieurs valeurs sont disponibles sous la zone Impact. Le niveau de gravité CVSS (Common Vulnerability Scoring System) s'affiche et contient une valeur comprise entre 1 et 10.

Étape 3 : renseignement des informations sur l'impact de la vulnérabilité

Gravité CVSS : _____

Plage : _____

Authentification : _____

Type d'impact : _____

L'en-tête suivant contient des liens avec des informations sur la faille et les solutions éventuelles s'y rapportant.

Étape 4 : rédaction d'une brève description de la solution trouvée sur ces pages à l'aide des liens hypertexte

_____

_____

_____

_____

_____

_____

_____

_____

Tâche 4 : remarques générales

Le nombre de failles sur les ordinateurs, réseaux et données continue d'augmenter. Les gouvernements ont consacré d'importantes ressources à la coordination et à la distribution des informations sur les failles et les solutions éventuelles. Il revient à l'utilisateur final d'implémenter la solution. Pensez à des solutions qui permettraient aux utilisateurs de renforcer la sécurité. Pensez aux habitudes des utilisateurs qui génèrent des risques de sécurité.

Tâche 5 : confirmation

Essayez de trouver une entreprise qui souhaite nous rencontrer pour expliquer comment les failles sont détectées et éliminées. Trouver une entreprise désireuse de le faire peut être difficile pour des raisons de sécurité, mais peut profiter aux participants, qui comprendront comment les failles sont éliminées dans le monde entier. Cela permettra également aux représentants de l'entreprise de rencontrer la classe et de mener des entretiens internes informels.