Travaux pratiques - Menaces pour la sécurité du réseau

Objectifs

Partie 1 : Découvrir le site web SANS

Partie 2 : Identifier les menaces pour la sécurité du réseau les plus récentes

Partie 3 : Décrire en détail une menace spécifique pour la sécurité du réseau

Contexte/scénario

Pour protéger un réseau contre les attaques, un administrateur doit identifier les menaces externes présentant un risque pour le réseau. Les sites web de sécurité peuvent être utilisés pour identifier les nouvelles menaces et pour fournir des options d'atténuation permettant de protéger un réseau.

L'un des sites les plus populaires et les plus fiables permettant de se défendre contre les menaces de sécurité affectant les ordinateurs et les réseaux est SysAdmin, Audit, Network, Security (SANS). Le site SANS offre plusieurs ressources, notamment une liste des 20 contrôles de sécurité essentiels pour une défense efficace sur Internet et le bulletin d'informations hebdomadaire @Risk: The Consensus Security Alert. Ce bulletin d'informations décrit en détail les nouvelles attaques réseau et vulnérabilités.

Dans ces travaux pratiques, vous visiterez et étudierez le site SANS, et vous l'utiliserez pour identifier les menaces de sécurité réseau récentes. Vous identifierez d'autres sites web identifiant les menaces, et vous étudierez et présenterez les détails d'une attaque réseau spécifique.

Ressources requises

- Périphérique avec accès Internet
- Ordinateur de présentation avec PowerPoint ou un autre logiciel de présentation installé

Partie 1: Découvrir le site web SANS

Dans la première partie, vous accédez au site web SANS et explorez les ressources disponibles.

Étape 1: Localisez les ressources SANS.

Accédez au site www.SANS.org. Dans la page d'accueil, mettez en surbrillance le menu **Resources** (Ressources).

Indiquez trois ressources disponibles.

Étape 2: Localisez les 20 principaux contrôles critiques.

Les **20 contrôles de sécurité essentiels pour une défense efficace sur Internet** (Twenty Critical Security Controls for Effective Cyber Defense) figurant sur le site web SANS sont l'aboutissement d'un partenariat impliquant le Department of Defense (DoD), la National Security Association, le Center for Internet Security (CIS) et le SANS Institute. La liste a été mise au point afin de hiérarchiser les contrôles de sécurité sur Internet et les coûts du DoD. Elle est devenue la pièce maîtresse des programmes de sécurité du gouvernement des États-Unis. Dans le menu **Resources** (Ressources), sélectionnez **Top 20 Critical Controls** (20 principaux contrôles essentiels).

Sélectionnez l'un de ces 20 contrôles essentiels et indiquez trois suggestions d'implémentation liées à ce contrôle.

Étape 3: Localisez le menu Newsletters (bulletins d'informations).

Sélectionnez le menu **Resources** (Ressources), sélectionnez **Newsletters** (Bulletins d'informations). Présentez brièvement chacun des trois bulletins disponibles.

Partie 2: Identifier les menaces pour la sécurité du réseau les plus récentes

Dans la deuxième partie, vous étudierez les menaces récentes pour la sécurité du réseau au moyen du site SANS et vous identifierez les autres sites contenant des informations sur les menaces de sécurité.

Étape 1: Localisez les bulletins d'informations archivés @Risk: Consensus Security Alert.

À partir de la page **Newsletters** (Bulletins d'informations), sélectionnez l'option **Archive** en regard de @RISK: The Consensus Security Alert. Faites défiler l'écran pour accéder aux **Archives Volumes** (Volumes des archives) et sélectionnez un bulletin d'informations hebdomadaire récent. Examinez les sections **Notable Recent Security Issues and Most Popular Malware Files** (Problèmes de sécurité récents et fichiers des programmes malveillants les plus populaires).

Citez quelques attaques récentes. Parcourez plusieurs bulletins d'informations récents, si nécessaire.

Étape 2: Identifiez les sites fournissant des informations récentes sur les menaces.

En plus du site SANS, identifiez d'autres sites web fournissant des informations récentes sur les menaces.

Citez quelques-unes des menaces de sécurité récentes détaillées sur ces sites web.

Partie 3: Décrire en détail une menace spécifique pour la sécurité du réseau

Dans la troisième partie, vous étudierez une attaque réseau spécifique, qui s'est déjà produite, et vous concevrez une présentation à partir de vos découvertes. Remplissez le formulaire ci-dessous en fonction de vos découvertes.

Étape 1: Remplissez le formulaire suivant pour l'attaque réseau sélectionnée.

Nom de l'attaque :	
Type d'attaque :	
Dates des attaques :	
Ordinateurs/entreprises concernés :	
Fonctionnement et description de ses actions :	
Options d'atténuation :	
Références et liens d'informations :	

Étape 2: Suivez les instructions du formateur pour terminer la présentation.

Remarques générales

1. Quelle procédure pouvez-vous suivre pour protéger votre propre ordinateur ?

2. Quelles sont quelques-unes des mesures importantes que les entreprises peuvent prendre pour protéger leurs ressources ?