Travaux pratiques – Menaces de sécurité réseau

Objectifs

1re partie : Découvrir le site Web SANS

- Accédez au site Web SANS et identifiez les ressources.

2e partie : Identifier les menaces de sécurité réseau les plus récentes

- Identifiez plusieurs menaces de sécurité réseau récentes en utilisant le site SANS.
- Identifiez les autres sites que SANS qui fournissent des informations sur les menaces de sécurité réseau.

3e partie : Décrire en détail une menace de sécurité réseau spécifique

- Sélectionnez une menace réseau récente spécifique et décrivez-la en détail.
- Présentez les informations à la classe.

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 menaces émergeantes 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, utiliserez le site SANS pour identifier les menaces de sécurité réseau récentes, examinerez d'autres sites Web identifiant les menaces, et 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

1re partie : Découvrir le site Web SANS

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

Étape 1 : Localisez les ressources SANS.

À partir de votre navigateur web, accédez à www.SANS.org. Dans la page d'accueil, mettez en surbrillance le menu **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. C'est devenu la pièce maîtresse de programmes de sécurité efficaces du gouvernement des États-Unis. Dans le menu **Resources** (Ressources), sélectionnez **Top 20 Critical Controls** (20 principaux contrôles essentiels).

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

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

Mettez en surbrillance le menu **Resources** (Ressources), sélectionnez **Newsletters** (Bulletins d'informations). Décrivez brièvement chacune des trois bulletins disponibles.

2e partie : Identifier les menaces de sécurité réseau les plus récentes

Dans la deuxième partie, vous étudierez les menaces de sécurité réseau récentes au moyen du site SANS et 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 et Most Popular Malware Files** (Problèmes de sécurité récents et Fichiers des programmes malveillants les plus populaires).

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

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

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

Énoncez quelques-unes des menaces de sécurité récentes détaillées sur ces sites Web.

3e partie : Décrire en détail une menace de sécurité réseau spécifique

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

Étape 1 : Remplissez le formulaire suivant pour l'attaque de 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 de l’instructeur 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 ?