ENG-406 - Sécurité des réseaux IP

Description

Ce programme de formation de 3 jours a pour but de fournir aux participants les outils nécessaires pour mettre en œuvre les mesures de sécurité associées aux réseaux à protocole Internet (IP). En étudiant les divers aspects de la sécurité de réseaux, les considérations architecturales et les technologies nécessaires pour accomplir ces tâches seront révélées.

Par l'entremise d'activités pratiques, le participant apprendra différentes façons d'accroître la sécurité dans le cadre d'un réseau IP.

Prérequis

Afin de profiter pleinement du contenu de ce programme de formation, il serait préférable que le participant ait suivi le programme de formation suivant ou acquis une expérience équivalente dans la matière :

- ENG-401F Introduction aux réseaux de données & au TCP/IP

Objectifs

- Décrire l'environnement de réseautage actuel et les défis afférents en matière de sécurité
- Identifier les cinq (5) piliers techniques et non techniques de la sécurité de réseau
- Présenter la façon de structurer une politique de sécurité et un processus de sécurité de réseau
- Présenter un aperçu de la cryptographie
- Caractériser les technologies de contrôle d'accès et d'authentification
- Expliquer comment efficacement accroître la sécurité des périmètres du réseau
- Définir les stratégies devant être adoptées pour améliorer la sécurité du réseau à l'interne
- Présenter les options disponibles pour améliorer la sécurité de l'information voyageant sur Internet

Sujets

Principes de base

- L'environnement de réseautage actuel
- Défis, objectifs et besoins en matière de sécurité
- Menaces et attaques potentielles
- Les cinq (5) piliers techniques et non techniques de la sécurité de réseau
- La première étape visant à bâtir un réseau mieux sécurisé : établir une politique de sécurité
- La prochaine étape visant à bâtir un réseau mieux sécurisé : mettre en œuvre un processus continu de sécurité de réseau

Cryptographie

- La nécessité de la cryptographie
- Définitions
- Chiffrement ou cryptage symétrique/asymétrique
- Modes de chiffrement
- Algorithmes de chiffrement
- Hachage
- Certificats numériques
- Gestion des clés

Technologies de contrôle d'accès et d'authentification, d'autorisation et de traçabilité (AAA)

- Définitions
- Méthodes et facteurs de contrôle d'accès et d'authentification
- Protocoles de contrôle d'accès et d'authentification : protocole d'authentification par mot de passe (PAP), protocole d'authentification par stimulation réponse ou Challenge-Handshake Authentication Protocol (CHAP), 802.1x, protocole d'authentification Extended Authentication Protocol (EAP)
- Protocoles d'authentification associés au serveur : protocole d'authentification Terminal Access Controller Access-Control System (TACACS/TACACS+), service d'authentification à distance des utilisateurs entrants (RADIUS), DIAMETER
- Authentification par jeton ou niveau supérieur : protocole Internet Protocol Security (IPSec), protocole Transport Layer Security (TLS) / Secure Sockets Layer (SSL), Kerberos

Défense des périmètres

- Situation dans son ensemble : définition, méthodes et restrictions/défis
- Pare-feux et filtres de paquets
- Mandataires
- Traduction des adresses réseau (NAT)
- Réseau Privé Virtuel (RPV)

Défense à l'interne

- Situation dans son ensemble : définition, méthodes et restrictions/défis
- Sécurité physique
- Segmentation du réseau à l'interne
- Certificats d'utilisateur
- Détection et prévention des intrusions
- Logiciel de détection et suppression de codes malveillants
- Contre-mesures décevantes

Améliorer la sécurité sur Internet

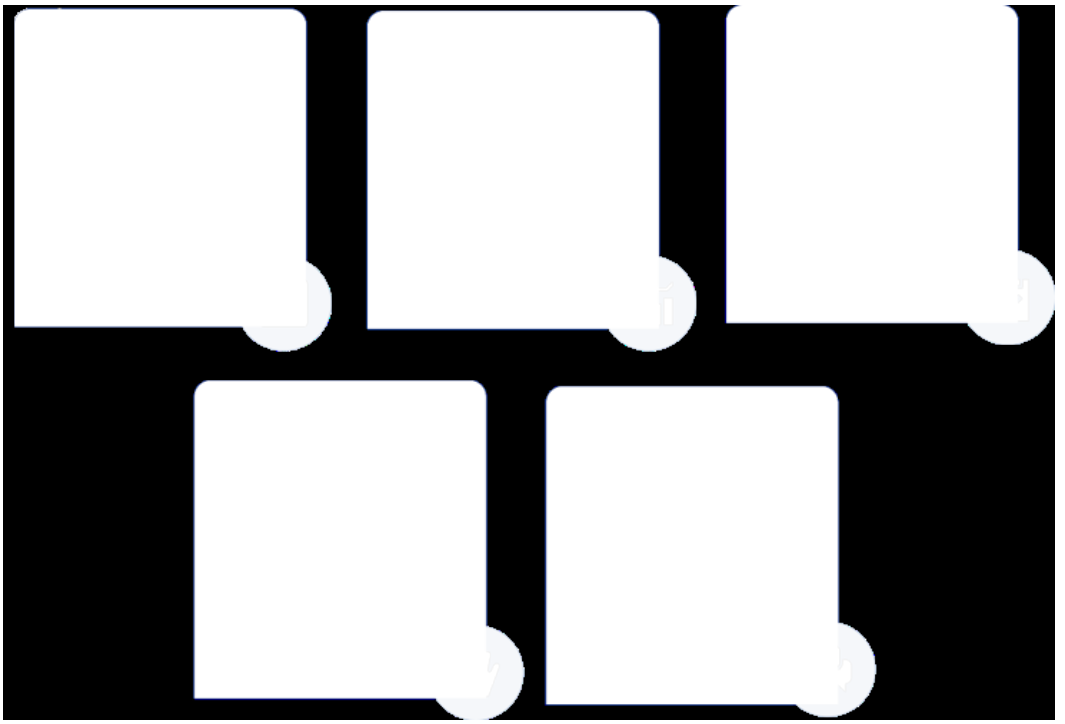
- Sécuriser le trafic sur le Web et les connexions à distance
- Sécuriser le trafic de courriel
- Sécuriser les transactions commerciales

Audience ciblée

- Personnel technique en ingénierie ou aux opérations souhaitant ou ayant besoin de parfaire sa compréhension en ce qui concerne l'amélioration de la sécurité des réseaux
- Gestionnaires techniques ou autres souhaitant élargir leur éventail de compétences en acquérant des connaissances en matière de sécurité de réseau

Méthodologie

Une combinaison d'activités pratiques et de présentations interactives pour favoriser et optimiser l'apprentissage :



Lieu

Certaines formations de Neotelis sont organisées dans différentes villes à travers le monde. Veuillez nous contacter à training@neotelis.com pour obtenir le Calendrier annuel de formation.



Neotelis peut également livrer des sessions de formation en intra-entreprise, spécialement pour votre organisation. Veuillez nous contacter à training@neotelis.com pour de plus amples informations et pour obtenir une Proposition.

À propos de Neotelis

Neotelis fournit des services de formation, de conseil ainsi que des conférences et des publications à l'industrie mondiale des télécommunications. Son équipe d'experts seniors a formé des milliers de dirigeants et gestionnaires travaillant pour des opérateurs, des régulateurs et des gouvernements dans plus de 120 pays à travers le monde.

4802 rue de Verdun, Bureau #1, Montreal, QC, H4G 1N1 Canada
Tel: +1 514 281 1211 Fax: +1 514 281 2005
info@neotelis.com