Sécurité défensive

VPN - Mise en oeuvre

3 jours (21h00) | ⭐⭐⭐⭐⭐ 5/5 | SEC-VPN | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 18/10/2024. Document téléchargé le 08/12/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Reconnaître les différentes caractéristiques et propriétés des principaux réseaux VPN
- Choisir le type de réseau VPN adapté aux attentes
- Monter un réseau VPN en s'appuyant sur des protocoles courants (SSL / TLS, PPTP, L2TP et IPsec)
- Diagnostiquer et résoudre les problèmes fréquemment rencontrés sur les réseaux VPN.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* *nous consulter pour la faisabilité en distanciel*

** *ratio variable selon le cours suivi*

Prérequis

Avoir des connaissances générales sur TCP/IP et la mise en oeuvre de services réseaux et systèmes.

Public concerné

Administrateurs système et réseau, techniciens système et réseau, consultants en sécurité.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Les fondamentaux

- Rappels sur le modèle OSI
- Le rôle du VPN
- Les différents types de VPN
- Les principaux protocoles
  - PPTP
  - L2TP
  - IPsec
  - SSL / TLS
  - OpenVPN
  - WireGuard...
- Les mécanismes de chiffrement et d'authentification
- Le PFS (Perfect Forward Secrecy)
- Choix du type de VPN en fonction des contraintes terrain
- La gestion des clés et des certificats
- Les stratégies de sécurité et de conformité réglementaire
- Les principaux produits communautaires et commerciaux

Exemples de travaux pratiques (à titre indicatif)

- *Citer des cas d'usage du VPN dans les entreprises des stagiaires*
- *Proposer des cas d'utilisation du VPN pour répondre à une problématique de confidentialité et d'intégrité*

Présentation et mise en oeuvre d'un VPN PPTP

- La structure d'un tunnel PPTP
- Les mécanismes de mise en oeuvre
- Les forces et faiblesses de PPTP
- L'implémentation de VPN PPTP
- Les tunnels PPTP et l'IPv6
- Les attaques et points de vigilance des VPN PPTP

Exemples de travaux pratiques (à titre indicatif)

- *Installation et paramétrage d'un serveur et d'un client VPN PPTP sous Windows ou Linux*
- *Capture de paquets encapsulés dans un tunnel PPTP et du canal de contrôle du VPN*

Jour 2

Présentation et mise en oeuvre d'un VPN L2TP

- Les composants d'un tunnel L2TP
- Les principes et mécanismes du L2TP
- Les forces et faiblesses du L2TP
- L'importance du protocole L2TPv3
- Les tunnels L2TP et l'IPv6

Exemples de travaux pratiques (à titre indicatif)

- *Installation et paramétrage d'un serveur et d'un client VPN L2TP sous Windows ou Linux*
- *Capture de paquets encapsulés dans un tunnel L2TP et du canal de contrôle du VPN*

Principe du protocole IPSec

- Rappels sur le chiffrement et l'authentification cryptographique
- Les AH (Authentification Header)
- Le protocole ESP (Encapsulating Security Payload)
- Le SAD (Security Association Database)
- Le protocole IKE (Internet Key Exchange)
- La SPD (Security Policy Database)
- L'AD (Authorization Database)

Exemples de travaux pratiques (à titre indicatif)

- *Mise en place d'un tunnel IPsec sous Windows ou Linux*
- *Ajout d'IPsec dans un tunnel L2TP*
- *Capture de paquets IPsec*

Jour 3

Principe du protocole TLS

- Description du protocole TLS
- Les différentes versions
- La structure d'un échange TLS
- Les particularités avec IPv6

Mise en oeuvre d'un VPN SSL / TLS

- Les différents types de VPN SSL / TLS
- Mise en oeuvre de portails Web
- Mise en oeuvre de portails applicatifs
- Les passerelles dédiées

Exemples de travaux pratiques (à titre indicatif)

- *Mise en oeuvre d'un VPN SSL / TLS sous Windows ou Linux*
- *Capture de trame VPN SSL / TLS et analyse de la phase d'établissement*

Troubleshooting

- Les méthodes pour établir un diagnostic
- Les méthodes d'analyse de trame et d'établissement du protocole d'enregistrement
- L'identification et la résolution des problèmes de connectivité
- La gestion des problèmes de performance
- Le dépannage des erreurs de configuration

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Accueil PSH.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.