Sécurité défensive

Investigation réseaux Wireshark

3 jours (21h00) | ★★★★½ 4,6/5 | SEC-INFRES | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

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

- Utiliser Wireshark pour capturer et analyser les paquets de données sur un réseau local ou distant
- Identifier les protocoles réseau courants (HTTP, HTTPS, FTP...) et leur structure de paquet
- Utiliser les fonctionnalités de filtrage, de recherche et de coloration de Wireshark pour cibler les paquets d'intérêt
- Repérer et diagnostiquer les problèmes de latence, de perte de paquets et de congestion sur un réseau
- Personnaliser l'interface de Wireshark et utiliser des dissecteurs heuristiques pour afficher les données de manière plus lisible
- Utiliser les tableaux et graphiques de Wireshark pour visualiser et interpréter les données de trafic
- Exporter les paquets de Wireshark vers d'autres outils d'analyse
- Utiliser Wireshark en ligne de commande pour capturer, fractionner et fusionner des paquets de données.

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 de base en réseaux de données : modèle OSI, protocoles TCP/IP, adresses IP, masques de sous-réseau... Aucune connaissance préalable de Wireshark n'est nécessaire.

Public concerné

Ingénieurs réseau, administrateurs système et professionnels de l'informatique souhaitant améliorer leurs compétences en matière d'analyse de réseau ou souhaitant découvrir les outils de diagnostic de réseau.

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

Introduction à Wireshark et aux réseaux de données

- Rappels et historique de Wireshark
- Modèle OSI et TCP/IP
- Supports de transmission et normes
- Format de trame
  - 802.3
  - 802.1Q
- Adresses réseau et encapsulation IP
- Protocoles :
  - ARP
  - ICMP
  - DHCP
  - DNS
  - HTTP / HTTPS
- TCP/IP et adressage applicatif
- En-tête TCP et la couche application
- Installation de Wireshark

Jour 2

Outils de Wireshark et analyse de trafic

- Comment Wireshark traite les paquets
- Eléments clés de Wireshark
- Suivre un paquet et analyser le trafic
- Personnaliser Wireshark
  - Colonnes
  - Dissecteurs...
- Repérer les problèmes de latence
  - TCP Delta

- Filtres de capture et capture de réseau sans fil
- Filtres d'affichage

Jour 3

Utiliser Wireshark pour construire et interpréter les données

- Filtres d'affichage avancés
- Colorer et exporter les paquets
- Construire et interpréter les tableaux et graphiques
- Réassembler le trafic et exporter les objets
- Ajout de commentaires
- Utilisation de Wireshark en ligne de commande
- Capture
- Fraction et fusion des paquets

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. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

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.