Développez vos talents
Certifiez vos compétences

Techniques avancées

Wireshark - Audit et dépannage du réseau

5 jours (35h00) | ★★★★½ 4,6/5 | WIR-AUD | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Réseaux et Télécoms › Techniques avancées

À l'issue de ce stage vous serez capable de :

- Mettre en oeuvre l'outil Wireshark
- Analyser les flux d'un réseau
- Diagnostiquer un problème réseau.

Niveau requis

Avoir de très bonnes connaissances réseaux.

Public concerné

Chefs de projets informatiques, ingénieurs, administrateurs et techniciens réseaux.

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.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les 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.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Jour 1

L'analyse réseau

- Définition
- Sécurité et analyse réseau
- Liste des tâches d'analyse
- Flux de trafic réseau

Exemple de travaux pratiques (à titre indicatif)

- *Analyser des trames types*

Wireshark

- Installation et maintenance
- Capture de paquets sur réseaux filaires et sans fil
- Prise en main

Exemples de travaux pratiques (à titre indicatif)

- *Installation de Wireshark*
- *Configuration du PC et des outils d'analyse*

Fonctionnalités Wireshark

- Définition de paramètres généraux et personnels
- Définition de valeurs de temps et d'interprétation de résultats
- Création et application de filtres d'affichage
- Suivi des flux et réassemblage de données
- Personnalisation du profil Wireshark
- Utilisation du système expert de Wireshark

Exemple de travaux pratiques (à titre indicatif)

- *Configuration des filtres et des profils*

Jour 2

Analyse du trafic standard

- L'analyse basique
- L'analyse TCP/IP
- L'analyse ARP
- L'analyse DHCP
- L'analyse DNS
- L'analyse HTTP
- L'analyse FTP

Exemple de travaux pratiques (à titre indicatif)

- *Capture et analyse des trames standards*

Jour 3

Analyse du trafic avancé

- L'analyse du trafic VoIP
- L'analyse du trafic Wi-Fi
- Graphiques IO

- Construction d'un modèle de référence
- Principales causes des problèmes de performance
- Analyse d'un trafic suspect
- Aperçu de l'infection d'un réseau

Exemple de travaux pratiques (à titre indicatif)

- *Capture et analyse des trames avancées*

Les outils de ligne de commande

- Intérêt des outils de ligne de commande
- Utilisation de Wireshark.exe
- Capture du trafic avec Tshark
- Listage des détails de fichiers de trace avec Capinfos
- Edition de fichiers de trace avec Editcap
- Fusion de fichiers de trace avec Mergecap
- Conversion de textes avec Text2cap
- Capture du trafic avec Dumpcap
- Rawshark

Exemple de travaux pratiques (à titre indicatif)

- *Capture et analyse via les commandes en lignes*

Jour 4

Préparation à la résolution des problèmes

- Utilisation de méthodes de dépannage efficaces
- Maîtrise des actions-clés du dépannage
- Utilisation d'une technique de capture correcte

Exemple de travaux pratiques (à titre indicatif)

- *Actions de dépannage*

Wireshark et la sécurité

- Les firewalls
- La détection d'intrusion
- Analyse Forensics
- Utilisation d'une technique de capture correcte

Exemple de travaux pratiques (à titre indicatif)

- *Analyse Forensics*

Jour 5

Dépannage basé sur les symptômes

- Résolution de problèmes Ethernet et Wi-Fi
- Focus sur les ralentissements réseaux et délais
- Identification de problèmes par l'utilisation du système Expert de Wireshark
- Identification d'erreurs d'application
- Optimisation de la détection d'un problème
- Désinfection d'un fichier de traces

Exemple de travaux pratiques (à titre indicatif)

- *Analyse des erreurs et délais*

Utilisation de Graphs pour détecter les problèmes

- Maîtrise basique et avancée des fonctions de Graph IO
- Graphs pour les problèmes de débit
- Graphs pour les problèmes de ralentissement
- Graphs sur les autres problèmes réseau

Exemple de travaux pratiques (à titre indicatif)

- *Configuration et analyse des Graphs*

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 ou une certification (M2i ou éditeur)