

Formation Wireshark, Prise en main

Présentation

Wireshark est un outil puissant pour l'analyse approfondie des réseaux, permettant d'identifier rapidement les problèmes de performance et de sécurité. Ce programme est conçu pour vous initier à l'utilisation de Wireshark afin d'examiner les protocoles réseau. Une fois les données capturées, elles peuvent être explorées via l'interface graphique de l'outil ou en mode ligne de commande avec tshark.

Durée : 21,00 heures (3 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

À la fin de cette formation, les participants seront capables de :

- Analyser les flux de données réseau.
- Appliquer des filtres et analyser les activités réseau.
- Rédiger des rapports d'analyse.
- Diagnostiquer les problèmes de performance à l'aide de Wireshark.

Prérequis

Des connaissances de base en TCP/IP sont requises pour suivre cette formation.

Public

Cette formation s'adresse aux administrateurs systèmes, administrateurs réseaux et développeurs.

Programme de la formation

Rappels des concepts fondamentaux

- Méthodes de communication réseau : unicast, multicast, broadcast.
- Topologies et gestion de l'accès. Modèle OSI.



- Structure d'une trame Ethernet : taille, signification (Runt, Giant...), protocole ARP.
- Protocoles de la couche 2 : 802.3, 802.1p, 802.1q, 802.1ad, multicast de couche 2.
- Format d'un paquet IP.
- Adresses spéciales : loopback, multicast (adresses connues), et méthodes de diffusion.
- Fonctionnement et analyse du protocole ICMP.

Découverte de l'interface Wireshark

- Exploration de la barre d'outils et de la zone de filtrage.
- Présentation de la zone d'affichage des paquets et de la vue hexadécimale du contenu.
- Compréhension de la barre d'état (mode expert, annotations, statistiques de capture, et profil actif).

Analyse des communications réseau avec Wireshark

- Capture du trafic réseau en texte clair (exemples : Telnet, HTTP).
- Identification des applications utilisées par des hôtes spécifiques.
- Établissement d'un point de référence pour l'analyse des communications.
- Vérification de l'état des services réseau.
- Détection des tentatives de connexion sur le réseau sans fil.
- Analyse du trafic inattendu et identification des communications en FTP, HTTP, ou VoIP.

Dépannage des réseaux avec Wireshark

- Identification des délais anormaux et des problèmes liés à TCP.
- Analyse des problèmes HTTP et des erreurs applicatives.
- Création de graphiques pour visualiser les problèmes.
- Détection de buffers saturés et d'adresses IP dupliquées.
- Résolution des problèmes liés au protocole DHCP ou aux relais DHCP.

Analyse de la sécurité réseau avec Wireshark

- Détection des applications utilisant des ports non standards.
- Identification du trafic provenant ou à destination d'hôtes suspects.
- Localisation des machines demandant une adresse IP.
- Repérage des processus de reconnaissance sur le réseau.
- Visualisation des adresses externes et de leurs emplacements géographiques.
- Analyse des conversations TCP/UDP entre clients et serveurs.
- Identification des signatures d'attaques réseau connues.

Organisation**Formateur**

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**En amont de la formation** (*évaluation en ligne dans l'extranet apprenant*)

- Recueil des besoins et des attentes des participants.

- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation (*évaluations en ligne dans l'extranet apprenant*)

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.