DOCAPOSTE Institute

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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- 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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- 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

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France