

Formation Wireshark, Analyse et diagnostic du trafic réseau

Présentation

Cette formation de 3 jours permet de maîtriser Wireshark, l'outil open source de référence pour l'analyse de paquets réseau. Elle s'adresse à toute personne amenée à surveiller, diagnostiquer ou auditer des communications réseau, dans un contexte de performance, de cybersécurité ou de support. À travers des exercices pratiques, les participants apprendront à capturer, filtrer, interpréter et exploiter efficacement les trames réseau.

Durée : 21,00 heures (3 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

À l'issue de la formation, les participants seront capables de :

- Comprendre le fonctionnement de Wireshark et de l'analyse réseau
- Capturer du trafic réseau en local ou à distance
- Filtrer les trames à l'aide de filtres d'affichage ou de capture
- Interpréter les échanges des principaux protocoles (ARP, DNS, HTTP, TCP, etc.)
- Identifier les anomalies, erreurs ou comportements suspects
- Utiliser Wireshark dans un contexte de diagnostic ou de cybersécurité

Prérequis

- Connaissance de base des protocoles réseau (TCP/IP, DNS, HTTP, etc.)
- Maîtrise des concepts fondamentaux de l'adressage IP et des modèles OSI/TCP-IP
- Expérience en administration système ou réseau recommandée

Public

- Administrateurs et ingénieurs réseau
- Techniciens support et exploitation IT
- Professionnels en cybersécurité (SOC, pentesters)



- Développeurs d'applications réseau ou embarquées
- Formateurs et enseignants en systèmes et réseaux

Programme de la formation

Jour 1 : Introduction à Wireshark et fondamentaux réseau

Introduction à l'analyse réseau : buts, usages, limites

- Installation et configuration de Wireshark (Linux / Windows)
- Rappels sur le modèle OSI, TCP/IP, encapsulation
- Types de trames, interfaces, modes de capture

Premières captures

- Choix de l'interface, options de capture
- Capture en direct vs analyse de fichiers .pcap
- Utilisation des filtres de capture et d'affichage
- Décryptage de trames : ARP, ICMP, IP, Ethernet

TP

- Capturer une séquence réseau locale, filtrer les paquets ARP et ICMP, analyser les échanges

Jour 2 : Analyse des protocoles de transport et applicatifs

Analyse des protocoles TCP et UDP

- Handshake, séquençage, retransmissions
- Flags, fenêtres, accusés de réception
- Reconstitution de flux (Follow TCP Stream)

Analyse de sessions DNS et DHCP

Analyse de protocoles applicatifs

- HTTP, HTTPS, FTP, SMTP

- Suivi de sessions utilisateur, lecture des requêtes/réponses
- Détection de lenteurs ou erreurs de connexion
- Introduction à l'analyse graphique : courbes d'I/O, latence, flux

TP

- Analyse complète d'un échange HTTP/TCP, détection d'un problème de lenteur réseau

Jour 3 : Diagnostic, sécurité et cas réels**Détection d'anomalies**

- Paquets malformés, retransmissions, collisions, TTL anormal
- Analyse de coupures, boucles, erreurs de configuration

Wireshark et cybersécurité

- Détection d'attaques simples (scan, spoofing ARP, DNS)
- Analyse de paquets suspects, recherche d'exfiltration

Captures avancées

- Filtres complexes, expressions logiques
- Suivi de conversation, couleurs, statistiques
- Export, partage et exploitation des fichiers .pcap
- Bonnes pratiques d'analyse et cas concrets (LAN, VoIP, Web, DNS)

TP final

- Étude de cas réaliste (diagnostic de panne réseau ou analyse post-incident)

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 compétence.

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 à 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.