EduGroupe
Accompagner pour réussir

Investigation réseaux Wireshark

Référence : **SECWSHARK** Durée : **3 jours (21 heures)** Certification : **Aucune**

Connaissances préalables

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

Profil des stagiaires

- Cette formation Wireshark s'adresse aux 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

Objectifs

- 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

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d’une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d’apports théoriques, d’exercices pratiques et de réflexions

Formateur·rice

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Jour 1

-

2. 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
- Adresses réseau et encapsulation IP
- Protocoles : ARP
- TCP/IP et adressage applicatif
- En-tête TCP et la couche application
- Installation de Wireshark

3. Jour 2

-

4. 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
- Repérer les problèmes de latence : TCP Delta
- Filtres de capture et capture de réseau sans fil
- Filtres d'affichage

5. Jour 3

-

6. 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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.