Wireshark – Les Fondamentaux

Date et durée

Code formation : WSK01FR
Durée : 4 jours
Nombre d'heures : 28 heures

Description

Wireshark est un logiciel libre d'analyse de paquets, utilisé notamment dans le dépannage et l'analyse des trafics de réseaux. Cette formation vous apprendra à maîtriser les fonctions de Wireshark pour une analyse en profondeur de vos réseaux et leurs dysfonctionnements.

Objectifs

A l'issue de cette formation le stagiaire aura une bonne maitrise de Wireshark pour une analyse en profondeur de tout ce qui transite sur le réseau et la détection des principales sources de dysfonctionnement des réseaux. Cette analyse se fera essentiellement sur Ethernet en mode filaire, IP, TCP et UDP ainsi que les protocoles majeurs utilisés en TCP/IP.

Pré-requis

Bonnes connaissances des réseaux Ethernet et TCP/IP

Public

Responsable du parc informatique

Cette formation s'adresse aux profils suivants

Administrateur système
Directeur des Systèmes d'Information (DSI)
Ingénieur système

Programme

- L'interface de Wireshark
- Comment capturer un flux réseau ?
- Création et utilisation de filtres de capture
- Gestion des préférences et des options de capture
- Coloration des trames pour séparer les flux
- Création et utilisation de filtres d'affichage
- Création de profils d'utilisation
- Sauvegarde et impression des captures
- Analyse du niveau 2 en Ethernet switché
- Analyse des flux ICMP

- Analyse des flux ARP
- Analyse des flux IP
- Analyse des flux UDP
- Analyse des flux TCP
- Analyse des flux applicatifs
    - DNS
    - DHCP
    - HTTP
    - FTP
- Statistiques et Graphiques
- Présentation des outils en lignes de commande
    - wireshark.exe
    - tshark.exe
    - dumpcap.exe
    - capinfos.exe
    - editcap.exe
    - mergecap.exe
    - text2cap.exe
    - rawshark.exe