



Wireshark : Audit, Dépannage et Administration du réseau

Lien :

<https://innov-systems.com/formation/wireshark-audit-depannage-et-administration-du-reseau>

 DURÉE
3 jours (21h)

 RÉFÉRENCE
RST34

 CATÉGORIE
**Audit Réseau
(Wireshark) et
Supervision des
Réseaux (Nagios,
Shinken, Zabbix)**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- ✓ Acquérir une bonne maîtrise 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

POUR QUI ?

- ✓ Responsable du parc informatique



Programme détaillé

1 / Introduction : Rappels

- Unicast, multicast, broadcast
- Les topologies et le contrôle d'accès
- OSI
- Format d'une trame Ethernet
- Tailles et signification (Runt, Giant...) et le protocole ARP
- Protocole de couche 2 (802.3, 802.1p, 802.1q, 802.1ad)
- Multicast de couche 2
- Format d'un paquet IP
- Les adresses particulières (loopback, APIPA,...)
- Les adresses de multicast
- Protocole ICMP

2 / L'analyse réseau

- Définition
- Sécurité et analyse réseau
- Liste des tâches d'analyse
- Flux de trafic réseau

3 / Wireshark

- Principes et fonctions de base
- Installation et maintenance
- Capture de paquets sur réseaux filaires et sans fil
- Présentation de l'interface de Wireshark

4 / Fonctionnalités Wireshark

- Paramètres généraux et personnels
- Valeurs de temps et d'interprétation de résultats
- Création et application de filtres d'affichage
- Suivi des flux et réassemblage de données
- Personnalisation du profil Wireshark
- Utilisation du système expert de Wireshark

5 / Les tâches d'analyse avec Wireshark

- Capture des communications réseaux en "clear text" (exemple Telnet, HTTP)
- Les applications utilisées par certains hôtes
- Définition d'un point de référence pour la communication réseau
- Vérification du bon fonctionnement de certains services du réseau
- Identifier qui veut se connecter au réseau sans fil
- Capture du trafic inattendu
- Capture et analyse du trafic d'un hôte ou d'un réseau
- Visualisation et rassemblement des fichiers transférés par FTP ou http
- Capture, visualisation et écoute des communications en VoIP

6 / Les tâches de dépannage avec Wireshark

- Identification des délais anormaux
- Identification des problèmes TCP
- Détection des problèmes HTTP
- Détection des erreurs applicatives
- Statistiques et Graphiques
- Identification des problèmes de buffer saturés
- Détection des problèmes d'adresse IP dupliquées
- Identification des problèmes liés au protocole DHCP ou au relai DHCP

7 / Analyse des menaces de sécurité sur les LAN

- Analyse de trafic en clair
- Analyse d'attaques de sniffing
- Analyse des techniques de reconnaissance réseau
- Détection des tentatives de craquage de mots de passe
- Autres attaques
- Outils complémentaires de Wireshark
- Filtres d'affichages importants

Approche pédagogique

- ✓ Support Ecrit et Projection
- ✓ Exposés Interactifs, Podcasts et Vidéos
- ✓ Brainstorming et Jeux de Rôle
- ✓ Cas Pratiques et Labs inclus pour leur impact opérationnel
- ✓ Test de Validation des Acquis des Connaissances

Prochaines dates programmées

 14 au 16 Oct. 2026

 Distanciel

 09 au 11 Déc. 2026

 Distanciel

 Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

 Téléphone : +212 522 247 210

 Email : contact@innov-systems.com

 Web : <https://www.innov-systems.com>