Audit et analyse des réseaux

★★★★★

AOC-19 **2 Jours (14 Heures)**

Description

Le trafic sur les réseaux de données est composé de nombreuses applications dont les volumes sont en général inversement proportionnels à l'importance qu'ils revêtent pour l'entreprise. Ce cours se propose de donner les clés, techniques et pratiques, de l'analyse des réseaux.

À qui s'adresse cette formation ?

Pour qui

Ce cours s'adresse aux architectes de réseaux, aux chefs de projets, aux responsables de systèmes d'information, aux ingénieurs réseaux.

Prérequis

Aucun.

Les objectifs de la formation

- Comprendre l'art d'analyser les flux réseau Connaitre les impacts de métrologie active et passive Identifier les outils utiles à la gestion du trafic Appréhender les méthodes d'audit appliqué à la sécurité Identifier les outils utiles pour surveiller la Qos

Programme de la formation

Les architectures de réseaux

- Rappels sur les architectures de protocoles.
- Le réseau d'entreprise, les réseaux virtuels, les techniques de VPN.
- Le réseau longue distance, les services des ISP.
- Les réseaux d'accès : xDSL, WiFi, WiMax.
- Les paramètres clés du réseau.
- Notion d'échantillonnage, problématiques de la mesure.
- Les débits, valeurs moyennes, rafales.
- Le nombre de paquets par seconde (PPS).
- L'analyse des goulets d'étranglement.

La métrologie

- Métrologie active vs métrologie passive.
- Métrologie : l'impact des couches du modèle en couches.
- Les approches purement réseau (niveau 2-3-4).
- Les approches applicatives (niveau 7).
- L'impact applicatif sur le réseau.
- Les groupes de l'IETF : IPSAMP, IPPM, IPFIX.
- Pourquoi tant d'efforts différents ? Les approches SNMP.
- Les corrélations statistiques.

La gestion du trafic

- Les outils.
- Les méthodes de contrôle d'admission.
- Impact des technologies sur les comportements.
- Capacity planning.
- Prévoir les évolutions.
- Garantir les performances.
- Des outils pour la gestion de parcs informatiques.
- Analyse des systèmes d'exploitation.
- Analyse des applications.
- Découverte de topologies.

La Sécurité

- Les principes de sécurité liés au trafic : les firewalls.
- Les approches Statefull et Stateless.
- Les limites des systèmes actuels.
- La détection d'intrusion : un audit en temps réel.
- La conformité du trafic aux règles du firewall.

La méthodologie

- Les étapes importantes.
- Pourquoi une méthodologie ? L'audit permanent.

La qualité de service

- Notions de SLA.
- QoS vs CoS.
- Le modèle de bout en bout.

Les outils d'audit et de Qos

- Les audits ponctuels.
- Pour quoi faire ? Exemple.
- Les performances et l'impact financier.
- Analyseurs, systèmes de gestion, Traffic Shapers, un état du marché.
- Acterna/Sniffer Pro.
- Ethereal/TCPDUMP.
- Qosmos.
- Qosmetrix.
- NetFlow, Ntop.
- Bilan et comparaison synthétique.