Techniques et Outils de Supervision de Réseaux

Date et durée

Code formation : RES60FR
Durée : 5 jours
Nombre d'heures : 35 heures

Description

Pour une sécurité optimale, un réseau doit être correctement supervisé par les protocoles et les formats de données SNMP.

Objectifs

Cette formation a pour objectif de se familiariser avec les protocoles et les formats de données SNMP (Simple Network Management Protocol), d'apprendre les techniques de flux de supervision de la sécurité réseau.

Pré-requis

Connaissances de base sur les réseaux et bases de TCP/IP

Public

Ce cours s'adresse aux administrateurs réseau et aux ingénieurs systèmes

Cette formation s'adresse aux profils suivants

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

Programme

1- Introduction à la supervision de réseau
Les problématiques de la surveillance des réseaux

- Architecture (réseaux, serveurs, clients)
- Hétérogénéité des systèmes et équipements
- Réseaux LAN & WAN…

Qu'est-ce que la supervision et le contrôle des réseaux?

- Que surveiller ?
- Quels outils ?

Les approches de supervision

- L'approche furtive
- L'approche coopérative

Les exemples d’approches dans des outils Open Source

- L'approche SNMP,
- L'approche OSI,
- Les approches propriétaires

2- Les outils d’observation des réseaux

- L'observation du trafic réseau
- L'approche quantitative et approche qualitative
- Les exemples d’outils (Wireshark, ntop)
- Les outils de supervision des performances réseaux (SmokePing)
- Les outils de test réseaux (Nmap)

3- Simple Network Management Protocol

- Historique : origines de SNMPv1
- Le paradigme Agent - Superviseur
- Les requêtes et les réponses SNMP
- Interrogation des agents vs. notifications spontanées
- Traps et notifications
- L'utilisation d’applications de supervision basées sur SNMP

4- Le Management Information Base et Structure of management Information

- La définition et l'identification des informations de gestions
- L'utilisation de ASN-1
- L'organisation des données en modules MIB
- MIB standards et MIB propriétaires

5- Les évolutions de SNMP

- La sécurité : Authentification et confidentialité
- La version 2c et la version 3

6- Les problèmes de mise en œuvre

- La version à utiliser
- Le paramétrage des équipements
- Agents et MIB supportées
- Les alarmes et les notifications
- Extension d’agents

7- Les applications de supervision

- Quelles applications utiliser?
- Les outils OpenSource vs. outils commerciaux
- Exemples d’applications de supervision (Munin, Nagios, Big Brother, OpManager)

8- Les travaux pratiques

- La planification, le paramétrage, et test d’un réseau
- La mise en œuvre pratique d’agents SNMP sur des systèmes (serveurs Windows et/ou Linux, switchs et routeurs)
- Interrogation en ligne de commandes, l'utilisation de MIB Browser
- L'analyse du codage des informations échangées
- L'analyse de MIB
- Le paramétrage de SNMP en version 1 et 2c
- L'utilisation de la sécurité de SNMPv3

- L'utilisation de Munin et SmokePing
- L'utilisation de Wireshark
- L'utilisation de Nmap
- La configuration et l'utilisation de NET-SNMP
- Les logiciels Open Source basés sur SNMP : MRTG, CACTI
- Les applications de supervision : Nagios, Big Brother, OpManager