26/03/2024

Réalisation professionnelle

Les bases du SNMP

ASSURMER

EVIEUX Lucas
BTS SIO SISR A2

I. Les bases du SNMP

L'objectif du SNMP est de surveiller le réseau et d'agir dès qu'une erreur se produit. Pour cela, il est nécessaire de contrôler :

- L'utilisation de la largeur de la bande
- L'état de fonctionnement des liens
- Les éventuels goulets d'étranglements
- Les problèmes de câblage
- Le bon cheminement de l'information entre les machines etc.

Pour cela, on utilise différents points stratégiques à observer tel que :

- Les routeurs,
- Les concentrateurs,
- Les liens, les postes,
- Les imprimantes.
- Borne Wi-Fi
- pfSense
- Etc ..

Le SNMP possède lui-même plusieurs composants, qui sont :

- **Les agents SNMP (port 161) :** chargés de superviser un équipement. Ils sont installés sur tout type d'équipement.

- **La station de supervision (manager, port 162) :** exécute les applications de gestion qui contrôlent les éléments réseau.

- **Le MIB (Management Information Base)** : collection d'objets résidant dans une base d'information virtuelle.

- **Le protocole :** permet à la station de supervision d'aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments.

Le SNMP possède également plusieurs versions :

Dans les versions 1 et 2, une requête SNMP contient un nom appelé communauté, associé à un mot de passe.

Sur de nombreux équipements, la valeur par défaut de communauté est public ou private.

Ces versions comportent de nombreuses lacunes de sécurité.

Les bonnes pratiques recommandent de n'utiliser que la version 3, cette dernière se basant sur le chiffrement DES avec deux mots de passe ou clés sur 64 bits partagés entre l'agent et le manager.