

LAB Pratique – Séance 2 : Sécurisation des connexions avec SSH

◆ Thème : "Sécuriser l'accès aux équipements de NovaTech"

Contexte pédagogique

Vous êtes missionné par la société **NovaTech** pour sécuriser l'accès à distance à ses équipements réseau. Cette entreprise a récemment souffert de connexions non autorisées via Telnet. Votre objectif : **configurer l'accès SSH sécurisé** sur un routeur et un switch, avec différents niveaux de privilèges pour les utilisateurs. Vous devez également appliquer les bonnes pratiques en termes de sécurité.

Infrastructure à mettre en place dans Packet Tracer

- 1 Routeur (R-Sec)
 - 1 Switch (SW-Core)
 - 1 PC Technicien (PC-Tech)
-

Câblage

- Connectez le PC au switch
 - Connectez le switch au routeur avec un câble droit
-

Objectifs du LAB

◆ Sur le routeur (R-Sec) :

- Renommez l'équipement
- Donnez-lui une IP (ex : 192.168.1.1 /24)
- Créez 2 comptes utilisateurs avec :
 - Un accès privilégié **niveau 15** (admin)
 - Un accès restreint **niveau 1 ou 0** (consultation uniquement)
- Configurez un nom de domaine et générez les clés RSA
- Activez uniquement SSH sur les lignes VTY
- Appliquez les paramètres suivants :

- Timeout à 60 secondes
- 3 tentatives de connexion max
- Version SSH v2 uniquement

◆ **Sur le switch (SW-Core) :**


- Renommez l'équipement
- Attribuez une IP à l'interface VLAN 1 (ex : 192.168.1.2 /24)
- Créez un utilisateur local avec privilège 15
- Activez SSH uniquement, identique au routeur

◆ **Sur le PC (PC-Tech) :**

- Testez la connexion SSH avec les deux utilisateurs (admin et restreint)
- Observez les différences de droits entre les comptes
- Essayez une commande interdite avec l'utilisateur restreint

 **Compétences travaillées**

- Configurer une interface VLAN avec IP
- Générer une clé RSA et activer SSH
- Créer des utilisateurs locaux avec différents privilèges
- Sécuriser les connexions distantes avec des paramètres avancés SSH
- Tester et analyser les résultats via terminal

 **Astuce :** pour tester rapidement les droits, utilisez show running-config avec les deux utilisateurs. Le compte restreint ne pourra pas y accéder !