

Projet : Device Security Hardening sur un Routeur VyOS

Étudiante : Bidzogo Caroline Suzanne

Introduction :

Ce projet vise à renforcer la sécurité d'un routeur VyOS à travers la désactivation des services vulnérables, la configuration d'un pare-feu, et l'activation de la journalisation.

1. Sécurisation des accès

Commande : `set system login user vyos authentication plaintext-password Fort@2024`

2. Activation du SSH

Commande :

`set service ssh`

`set service ssh port 22`

3. Suppression des services non sécurisés

Commande :

`delete service telnet`

`delete service ftp`

`delete service http`

4. Configuration du pare-feu

Commandes :

`set firewall name WAN-IN default-action drop`

`set firewall name WAN-IN rule 10 action accept`

`set firewall name WAN-IN rule 10 protocol tcp`

set firewall name WAN-IN rule 10 destination port 22

set firewall name WAN-IN rule 10 state new enable

set interfaces ethernet eth0 firewall in name WAN-IN

5. Blocage des pings ICMP (optionnel)

Commande : set firewall name WAN-IN rule 20 action drop

6. Journalisation

Commande : set system syslog global facility all level info

7. Vérification via Nmap

Commande : nmap -sS <ip_vyos>

Conclusion :

Ces étapes permettent de durcir la configuration par défaut de VyOS et de sécuriser les accès réseau.