MSCYBER#04 - Sécurité des accès distants sur les architectures hybrides

En tant que administrateur Infrastructure Sécurisée, vous devez préparer un modèle de fichier de configuration pour sécuriser les connexions distantes sur les serveurs GNU/Linux de l'entreprise, qu'ils soient hébergés en propre par l'entreprise ou dans le cloud.

Authors

Roblot Jean-Philippe - jroblot.simplon@proton.me
Drula Kevin - k.drula.simplon@proton.me

Version

10/01/2024 - V1R0

Releases

Powered by https://shields.io

1. PREPARATION

Installation d'une machine virtuelle Ubuntu Server via VirtualBox
Carte réseau en mode Pont
TCP/IP statique 192.168.1.1xx (xx étant la valeur de l'ip de la machine hôte)

Machine serveur

- GNU/Linux/UBUNTU Server LTS 22.04
- vCPU : 2 core
- vRAM 8Go
- vHDD : 40Go
- @ip : 192.168.1.162/24
- Port SSH : 22

Machine client

- Laptop Windows 10 Pro Version 22h2
- Nom : GDO-PC-PF1M1RXE
- CPU : 6 core
- RAM 32Go
- SSD : 512Go
- Invite de commande - OpenSSH

Mise à jour de la machine serveur

```
sudo apt update # charge le catalogue de maj
sudo apt upgrade # effectue la mise à jour
```

Configuration de l'ip fixe

```
sudo nano /etc/netplan/00-installation-config.yaml

network:
  ethernets:
    enp0s3:
       addresses: [192.168.1.200/24]
       routes:
           - to: default
             via: 192.168.1.1
       nameservers:
           addresses: [8.8.8.8, 8.8.4.4]
       dhcp4: false
       dhcp6: false
  version: 2
```

Tester et aplliquer la configuration

```
sudo netplan try
sudo netplan apply
```

Installation OpenSSH sur le serveur

```
sudo apt install openssh-server
```

Effectuer une sauvegarde du fichier de configuration par défaut d'OpenSSH et retirer les droits d'écriture

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

Identifier la configuration par défaut

```
nano /etc/ssh/sshd_config
```

Tester notre configuration serveur en établissant une connexion SSH depuis notre machine client

Activités

- SEC02 - Interdire l'authentification par mot de passe :
  1 - Décommenter la ligne 'PasswordAuthentification' et lui affecter la valeur 'no'
  2 - Commenter la ligne 'Include /etc/ssh/sshd_config.d/*.conf'
- SEC04 - Imposer le port 666 pour les connexions au serveur :
  décommenter la ligne 'Port' et lui affecter la valeur 666