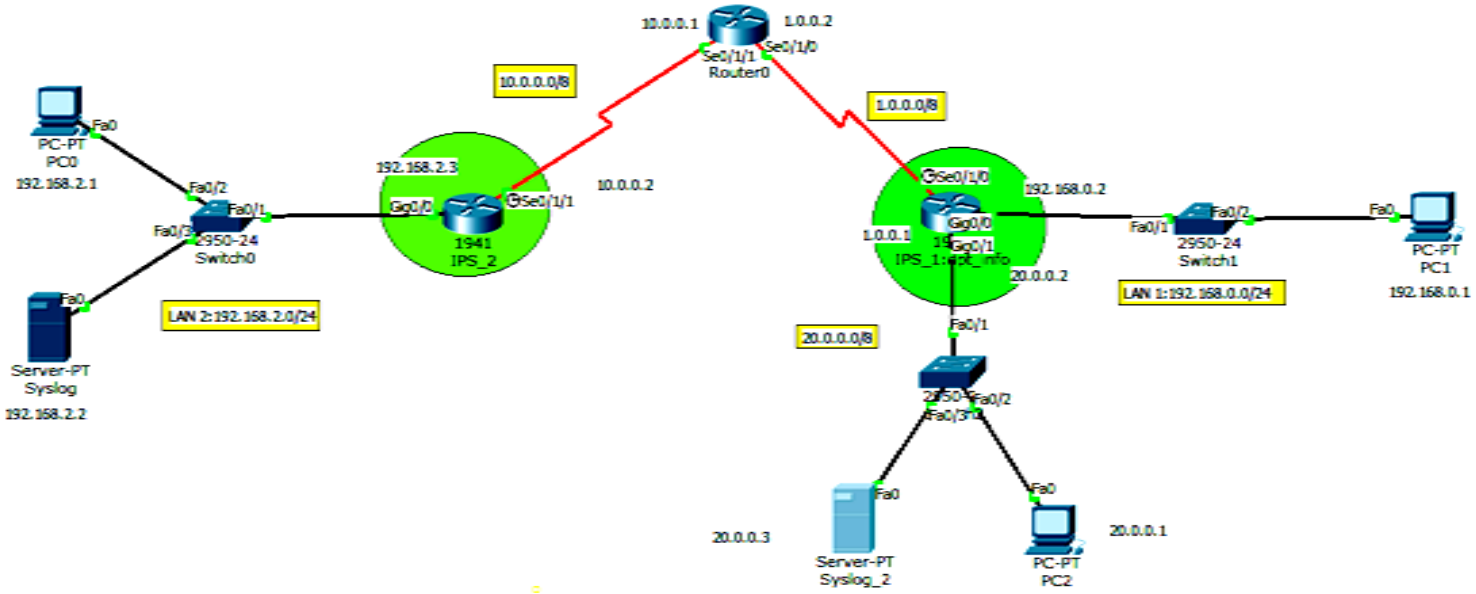
Sécurité informatique (MGL-1)

TP 2: Configuration des IPS basés sur la signature

Ce TP consiste à configurer un **IPS** sur le routeur (dpt_info) pour analyser le trafic entrant sur le réseau 192.168.2.0/24 et 20.0.0.0/8 . Le serveur est utilisé pour enregistrer les messages IPS (les messages journaux (Syslog)).

Recommandations:

- Réalisez la topologie ci-dessous en configurant les adresses IP pour chaque équipement.
- Tester la connectivité entre PC0, PC1 et le serveur.
- Réglez : heure et date dans les messages syslog (pour surveiller le réseau en temps réel).
- Réglez l'horloge et configurez le service d'horodatage pour la connexion aux routeurs.
- Activez IPS pour produire une alerte et abandonner les paquets de réponse d'écho ICMP (ID:2004) en ligne.



<u>Objectifs de ce TP est:</u>

1- Activez IOS IPS.
2- Configurez logging.
3- Modifiez la signature de l'IPS.
4- Vérifiez l'IPS.

1- Pour le réseau 20.0.0.0/8

Partie I: Activez IOS IPS

Étape 1 : Activez le package (Security Technology)

1- Sur le retour **dpt_info**, écrivez la commande **show version (Router#show license feature)** pour afficher les informations de licence du package **Security Technology**.

2- Si le package Security Technology n'a pas été activé, utilisez la commande suivante pour activer le package.**dpt_info(config)# license boot module c1900 technology-package securityk9**

3- Acceptez le contrat de licence (**yes**).

4- Enregistrez la configuration en cours (**W**) et redémarrer le routeur (**reload**) pour activer la licence de sécurité.

5- Vérifiez que le package Security Technology a été activé en utilisant la commande **show version (Router#show license feature)**.

Étape 2: Créez un répertoire de configuration IOS IPS.

Sur le retour **dpt_info**, créez un répertoire pour le sauvegarde à l'aide de la commande **mkdir**. Nommez le répertoire **ipsdir**.

```
dpt_info# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir  // pour verifier
ecrire la commande « dir »
```

Étape 3: Configurez l'emplacement de stockage des signatures IPS.

Toujours sur le retour **dpt_info**, configurez l'emplacement de stockage de la signature IPS pour qu'il soit le répertoire que vous venez de créer « **ipsdir** ».

```
dpt_info(config)# ip ips config location ipsdir
```

Étape 4: Créez une règle IPS.

Sur le retour **dpt_info**, en mode de configuration globale, créez un nom de règle IPS à l'aide de la commande ***ip ips*** et donner le nom **iosips**.

```
dpt_info(config)# ip ips name iosips
```

Étape 5: Configurez logging.

En cas d'attaque l'IPS envoie les messages au serveur Syslog.

1- Activez syslog.

```
dpt_info(config)# ip ips notify log
```

2- Si nécessaire, utilisez la commande **clock set** pour réinitialiser l'horloge.

```
dpt_info# clock set 23:10:00  18 february 2023
```

3- Vérifiez que le service d'horodatage pour loggin est activé sur le routeur à l'aide de la **commande show run**. Activez le service d'horodatage s'il n'est pas activé.

```
dpt_info(config)# service timestamps log datetime msec
```

4- Envoyez les messages du journal au serveur syslog à l'adresse IP 20.0.0.3

```
dpt_info(config)# logging host 20.0.0.3
```

Étape 6: Configurez IOS IPS pour utiliser les catégories de signature.

- Retirez (arrêter) les catégories pour toutes les signatures avec la commande « `retired true` »
- Annulez le retrait de la catégorie IOS_IPS Basic avec la commande « `retired false` »

```
dpt_info(config)# ip ips signature-category
dpt_info(config-ips-category)# category all
dpt_info(config-ips-category-action)# retired true
dpt_info(config-ips-category-action)# exit
dpt_info(config-ips-category)# category ios_ips basic
dpt_info(config-ips-category-action)# retired false
dpt_info(config-ips-category-action)# exit
dpt_info(config-ips-cateogry)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Étape 7: Appliquez la règle IPS à une interface.

```
dpt_info(config)# interface g0/1
dpt_info(config-if)#ip ips iosips out   // interface sortante
```

Partie 2: Modifier la signature

Étape 1: Modifier « event-action » d'une signature.

Annulez le retrait de la signature de la demande d'écho (signature 2004, ID de sous-signalisation 0), activez-la et modifiez l'action de signature en alerte et suppression.

```
dpt_info (config)# ip ips signature-definition
dpt_info(config-sigdef)# signature 2004 0
dpt_info(config-sigdef-sig)# status
dpt_info(config-sigdef-sig-status)# retired false
dpt_info(config-sigdef-sig-status)# enabled true
dpt_info(config-sigdef-sig-status)# exit
dpt_info(config-sigdef-sig)# engine
dpt_info(config-sigdef-sig-engine)# event-action produce-alert
dpt_info(config-sigdef-sig-engine)# event-action deny-packet-inline
dpt_info(config-sigdef-sig-engine)# exit
dpt_info(config-sigdef-sig)# exit
dpt_info(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Étape 2: Utilisez les commandes show pour vérifier IPS.

Utilisez la commande **show ip ips all** pour afficher le récapitulatif de l'état de la configuration IPS. A quelles interfaces et dans quel sens s'applique la règle **iosips** ?

Étape 3: Vérifiez que l'IPS fonctionne correctement (pinger les PCs).

Étape 4: Affichez les messages syslog.

1- Cliquez sur Syslog du serveur .
2- Sélectionnez l'onglet Services.
3- Sélectionnez SYSLOG pour afficher le fichier jour.

Étape 5 : Vérifier les résultats.

2- Pour le réseau 192.168.2.0/24

- **Refaire les mêmes étapes de configuration pour le réseau 192.168.2.0**