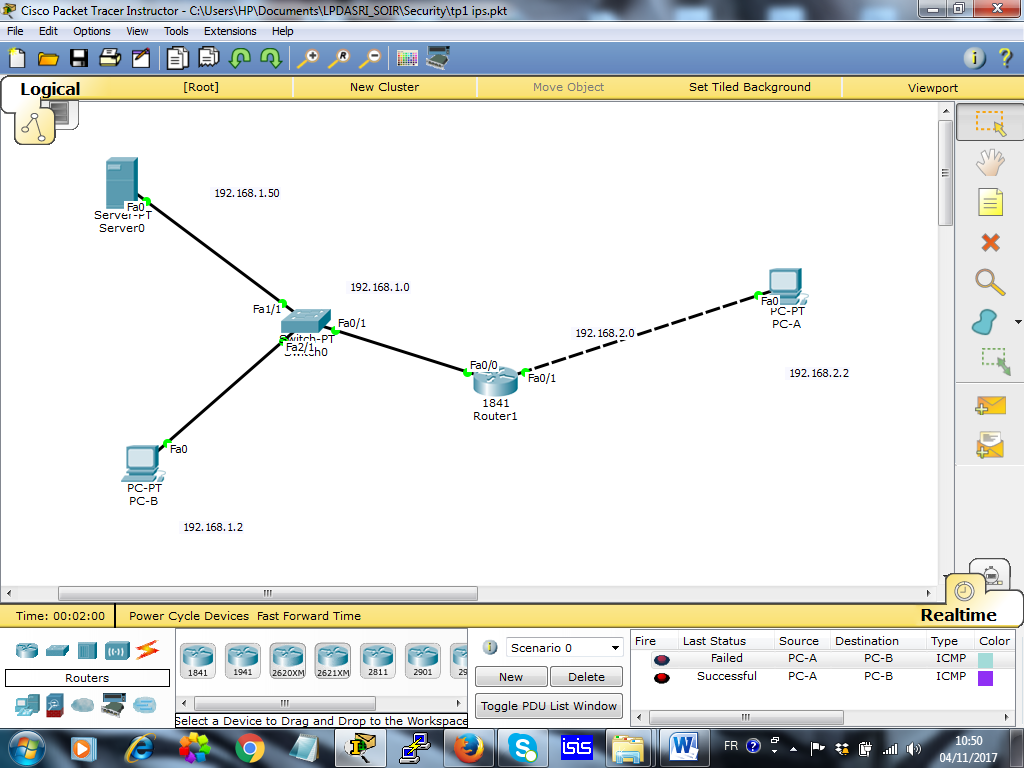
Travaux pratiques : Réalisation d’un IPD/IDS

**TP :1**



PT Activity: Configure IOS Intrusion Prevention System (IPS) using CLI (invite de commande) :

L’objectif est d’installer un IPS qui détecte les tentatives d’accès à un réseau (ici 192.168.1.0) et d’envoyer les notifications à un serveur sysLog.

Pour cette raison nous allons construire deux réseaux connectés via un routeur, le premier réseau contient un PC-A, le deuxième réseau contient un PC-C et un serveur.

**Tâche 1 :**

* Choisir un routeur 1841
* Renommer le routeur :

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#host

Router(config)#hostname R1

R1(config)#

* Configurer l’interface fast0/0 par l’adresse 192.168.1.1 et activer cette interface.
* Configurer l’autre interface fast0/1 par l’adresse 192.168.2.1 et l’activer
* Configurer le PC-A par l’adresse 192.168.1.2
* Configurer le serveur dans le même réseau par l’adresse 192.168.1.50
* Configurer le PC-C par l’adresse 192.168.2.2

**Tâche 2:** **Verify network connectivity.**

·    **Ping** from PC-C to PC-A. The ping should be successful.

·    **Ping** from PC-A to PC-C. The ping should be successful.

**Tâche 3:** **Create an IOS IPS configuration directory in flash.**

* Utiliser la commande suivante pour créer un répertoire dans la mémoire flash :

R1#mkdir ipsdir

* On R1, configure the IPS signature storage location to be the directory you just created.

R1(config)#ip ips config location ipsdir

* On R1, create an IPS rule name using the **ip ips name***name*command in global configuration mode. Name the IPS rule **iosips**.

R1(config)#ip ips name iosips

Send log messages to the Syslog server at IP address 192.168.1.50.

R1(config)#service timestamps log datetime msec

R1(config)#logging on

R1(config)#logging 192.168.1.50

R1(config)#ip ips notify log

Retire the **all** signature category with the **retired true** command (all signatures within the signature release). Unretire the **IOS\_IPS Basic** category with the **retired false** command.

R1(config)#ip ips signature-category

R1(config-ips-category)#category all

R1(config-ips-category-action)#retired true

R1(config-ips-category)#category ios\_ips basic

R1(config-ips-category-action)#retired false

**Apply the IPS rule to an interface:**

R1(config)#int fa0/0

R1(config-if)#ip ips iosips out

**Change the event-action of a signature.**

Un-retire the echo request signature (signature 2004, subsig ID 0), enable it and change the signature action to alert, and drop.

R1(config)#ip ips signature-definition

R1(config-sigdef)#signature 2004 0

R1(config-sigdef-sig)#status

R1(config-sigdef-sig-status)#retired false

R1(config-sigdef-sig-status)#enabled true

R1(config-sigdef-sig-status)#exit

R1(config-sigdef-sig)#engine

R1(config-sigdef-sig-engine)#event-action produce-alert

**Use show commands to verify IPS.**

Use the **show ip ips all** command to see an IPS configuration status summary.

To which interfaces and in which direction is the iosips rule applied?

**Verify that IPS is working properly.**

From PC-C, attempt to **ping** PC-A. Were the pings successful? Why or why not?

From PC-A, attempt to **ping** PC-C. Were the pings successful? Why or why not?

**View the Syslog messages.**

Click on the **Syslog** server. Select the**Config**tab. In the left navigation menu, select**SYSLOG** to view the log file.

