Centre Universitaire de Mila

Institut des Sciences et de la Technologie

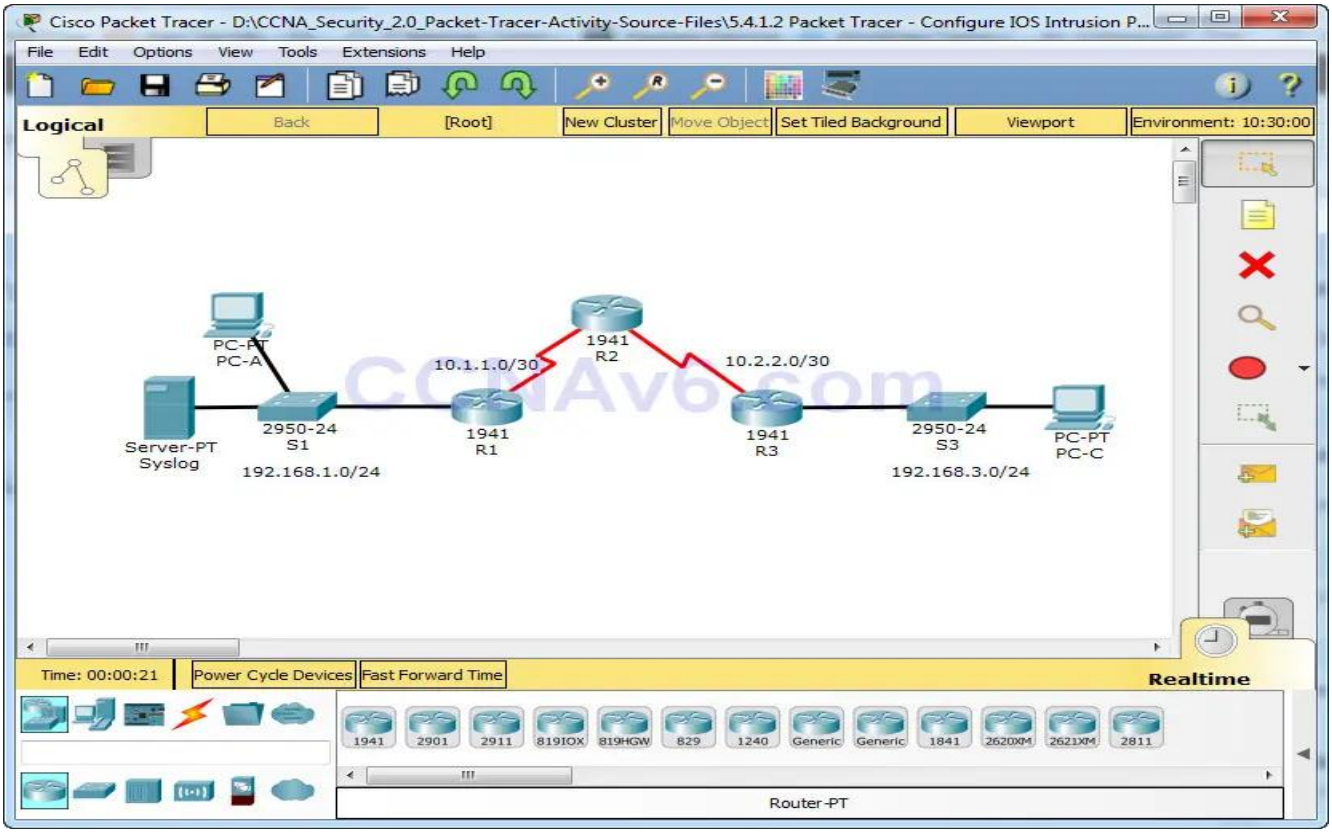
Master I I2A

Matière: sécurité des réseaux

TP 3 : IDS/IPS

Packet Tracer – Configurer le système de prévention des intrusions (IPS) IOS à l'aide de l'interface de ligne de commande

Topologie



Objectifs

• Activer IOS IPS.

• Configurer la journalisation.

• Modifier une signature IPS.

• Vérifiez IPS.

Contexte / Scénario

Votre tâche consiste à activer IPS sur R1 pour analyser le trafic entrant dans le réseau 192.168.1.0.

Le serveur intitulé Syslog est utilisé pour consigner les messages IPS. Vous devez configurer le routeur pour identifier le serveur syslog qui recevra les messages de journalisation. L'affichage de l'heure et de la date correctes dans les messages syslog est essentiel lors de l'utilisation de syslog pour surveiller le réseau. Réglez l'horloge et configurez le service timestamp pour la journalisation sur les routeurs. Enfin, activez IPS pour produire une alerte et supprimer les paquets de réponse d'écho ICMP en ligne.

Partie 1: Activer IOS IPS

Remarque : Dans Packet Tracer, les routeurs ont déjà les fichiers de signature importés et en place.

Étape 1 : Activez le package Security Technology.

a. Sur R1, exécutez la commande show version pour afficher les informations de licence du package technologique.

b. Si le package Security Technology n'a pas été activé, utilisez la commande suivante pour activer le package.

R1(config)# license boot module c1900 technology-package securityk9

c. Accepter le contrat de licence de l'utilisateur final.

d. Enregistrez la configuration en cours d'exécution et rechargez le routeur pour activer la licence de sécurité.

e. Vérifiez que le package Security Technology a été activé à l'aide de la commande show version.

Étape 2 : Vérifiez la connectivité réseau.

a. Ping de PC-C à PC-A. Le ping devrait réussir.

b. Ping de PC-A à PC-C. Le ping devrait réussir.

Étape 3: Créez un répertoire de configuration IOS IPS dans flash.

Sur R1, créez un répertoire dans Flash à l'aide de la commande mkdir. Nommez le répertoire ipsdir.

R1# mkdir ipsdir

Create directory filename [ipsdir]? <Enter>

Created dir flash:ipsdir

Étape 4 : Configurez l'emplacement de stockage des signatures IPS.

Sur R1, configurez l'emplacement de stockage des signatures IPS pour qu'il soit le répertoire que vous venez de créer

R1(config)# ip ips config location flash:ipsdir

Étape 5 : Créez une règle IPS.

Sur R1, créez un nom de règle IPS à l'aide de la commande **ip ips name** en mode de configuration globale. Nommez la règle IPS iosips.

R1(config)# ip ips name iosips

Étape 6 : Activez la journalisation.

IOS IPS prend en charge l'utilisation de syslog pour envoyer une notification d'événement. La notification Syslog est activée par défaut. Si la console de journalisation est activée, les messages du syslog IPS s'affichent.

a. Activez syslog s'il n'est pas activé.

R1(config)# ip ips notify log

b. Si nécessaire, utilisez la commande de réglage de l'horloge à partir du mode EXEC privilégié pour réinitialiser l'horloge.

R1# clock set 10:20:00 10 january 2014

c. Vérifiez que le service timestamp pour la journalisation est activé sur le routeur à l'aide de la commande show run. Activez le service timestamp s'il n'est pas activé.

R1(config)# service timestamps log datetime msec

d. Envoyer des messages de journal au serveur syslog à l'adresse IP 192.168.1.50.

R1(config)# logging host 192.168.1.50

Étape 7 : Configurez IOS IPS pour utiliser les catégories de signature.

Retirez la catégorie all signature avec la commande **retired true** (toutes les signatures dans la libérerais de signature). Annulez le retrait de la catégorie IOS_IPS Basic avec la commande **retired false** .

R1(config)# ip ips signature-category

R1(config-ips-category)# category all

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

R1(config-ips-category-action)# exit

R1(config-ips-category)# category ios_ips basic

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

R1(config-ips-category-action)# exit

R1(config-ips-cateogry)# exit

Do you want to accept these changes? [confirm] <Enter>

Étape 8 : Appliquez la règle IPS à une interface.

Appliquez la règle IPS à une interface à l'aide de la commande **ip ips name direction** en mode de configuration d'interface. Appliquez la règle sortante sur l'interface G0/1 de R1. Après avoir activé IPS, certains messages de journal sont envoyés à la ligne de console indiquant que les moteurs IPS sont en cours d'initialisation.

Remarque : La direction **in** signifie que IPS inspecte uniquement le trafic entrant dans l'interface. De même, **out** signifie que IPS inspecte uniquement le trafic sortant de l'interface.

R1(config)# interface g0/1

R1(config-if)# ip ips iosips out

Partie 2 : Modifier la signature

Étape 1 : Modifier l'événement-action d'une signature.

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

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

R1(config-sigdef-sig-engine)# event-action deny-packet-inline

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

R1(config-sigdef-sig)# exit

R1(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 résumé de l'état de configuration IPS.

À quelles interfaces et dans quel sens la règle iosips est-elle appliquée ?

Étape 3 : Vérifiez que IPS fonctionne correctement.

a. À partir de PC-C, essayez d'envoyer un ping à PC-A. Les pings ont-ils été réussis ? Expliquer.

b. à partir de PC-A, essayez d'envoyer un ping à PC-C. Les pings ont-ils été réussis ? Expliquer.

Étape 4 : Affichez les messages syslog.

a. Cliquez sur le serveur Syslog.

b. Sélectionnez l'onglet Services.

c. Dans le menu de navigation de gauche, sélectionnez SYSLOG pour afficher le fichier journal.

Exercice 1 : Questions de cours

1. Donner la définition d'un IDS et d'un IPS. Quelle est la différence essentielle entre les deux ?
2. Pourquoi dit-on qu'un IDS est un dispositif passif alors qu'un IPS est un dispositif actif ?
3. Citer trois formes physiques sous lesquelles un IDS/IPS peut être déployé dans un réseau.
4. Quels sont les composants matériels minimaux d'un IDS dédié ? Justifier la présence de chacun.
5. Expliquer pourquoi tout le trafic doit obligatoirement traverser un IPS, ce qui n'est pas le cas pour un IDS.

Exercice 2 : Vrai / Faux (justifier)

- Un IDS peut bloquer une attaque en cours.
- Un IPS peut créer un goulot d'étranglement dans le réseau.
- Un IDS placé en mode passif analyse une copie du trafic.
- Un IPS et un firewall ont exactement le même rôle.
- Une signature peut décrire à la fois un seul paquet ou une suite de paquets.

Exercice 3 : Signature atomique vs composite

1. Définir la signature atomique et la signature composite. Donner les avantages et inconvénients de chacune.
2. Pour chacune des situations suivantes, indiquer s'il s'agit d'une signature atomique ou composite :

- Un paquet TCP avec les drapeaux SYN et FIN activés simultanément.
- Trois tentatives de connexion SSH échouées en moins de 10 secondes depuis la même IP.
- Un paquet ICMP de taille supérieure à 65 535 octets.
- Une séquence : requête HTTP GET → 401 → GET → 401 → GET → 200 sur la même URL.
- Un paquet UDP destiné au port 31337.

Exercice 4 : Comparaison des méthodes

Compléter le tableau comparatif suivant entre Pattern-based detection et Anomaly-based detection : Principe, Détection des attaques 0-day, Taux de faux positifs, Mécanisme d'apprentissage, Consommation de ressources, Difficulté de configuration

Exercice 5 : Faux positifs / Faux négatifs

1. Définir précisément les notions de faux positif et faux négatif pour un IDS.
2. Lequel des deux est le plus dangereux du point de vue de la sécurité ? Justifier.
3. Lequel est le plus gênant du point de vue opérationnel pour l'administrateur ?

Exercice 6 : Types d'IDS

Comparer NIDS (Network-based), HIDS (Host-based) et Application-based IDS selon les critères suivants : portée, performances, capacité à détecter les liaisons cryptées, vulnérabilité du détecteur lui-même.

Exercice 7 : Placement d'un IDS

Une entreprise possède l'architecture suivante : Internet — Routeur — Firewall — Réseau interne, avec deux DMZ (DMZ1 hébergeant les serveurs Web/FTP publics, DMZ2 hébergeant les serveurs de messagerie internes).

1. Proposer un schéma de placement de plusieurs IDS répondant aux objectifs suivants : détection des attaques externes, protection des serveurs publics, détection des attaques internes.
2. Pour chaque détecteur placé, justifier son emplacement et indiquer le type d'attaques qu'il pourra détecter.
3. Quels sont les inconvénients d'un IDS placé exclusivement à l'extérieur du firewall ?
4. Quels sont les avantages d'un IDS placé sur les segments DMZ ?