SISR 4-5

Pacôme MASSOL

2016-2017
4.0

Table des matières

Cours : Systèmes de Détection d'Intrusion (IDS)

1. Qu'est-ce qu'un IDS ?

Wikipedia définit ainsi cette famille d'outils réseau :

Définition : IDS (Intrusion Detection System)

Mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

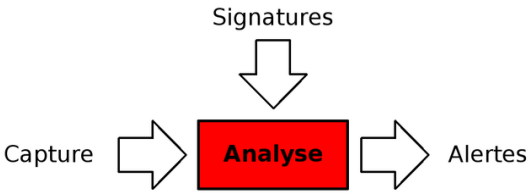
Il existe trois grandes familles d'IDS :

- NIDS (*Network-based Intrusion Detection System*) : plate-forme indépendante qui identifie les intrusions en examinant le trafic réseau. Dans un NIDS, des capteurs sont placés à des points stratégiques du réseau à surveiller, souvent dans la zone démilitarisée (DMZ) ou aux frontières du réseau. Ils capturent tout le trafic réseau et analysent le contenu des paquets pour repérer du trafic malveillant. Un exemple de NIDS est Snort.
- HIDS (*Host-based Intrusion Detection System*) : se compose d'un agent installé sur un hôte et qui identifie les intrusions en analysant les appels système, les journaux d'applications, modifications sur le système de fichiers (exécutables, fichiers de mots de passe, bases de donnée, listes de contrôle d'accès, etc). Des exemples de HIDS sont Tripwire et OSSEC.
- IDS hybrides : utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes.

2. Comment fonctionne un IDS ?

Nous nous intéressons ici aux NIDS, qui d'une certaine manière, fonctionnent comme un antivirus mais à un niveau OSI plus bas puisqu'ils travaillent au niveau IP, TCP/UDP et des protocoles applicatifs (HTTP, SMTP, etc.).

Les NIDS fonctionnent selon ce schéma :



source : wikipedia

3. Capture du trafic

La capture se fait trame par trame sur le modèle de Wireshark (d'ailleurs, cela repose généralement sur la même librairie *libpcap*). Il faut parfois rassembler les n trames Ethernet constituant une conversation TCP.

4. Analyse

4.1. Base de signatures

L'IDS utilise une base de données de "modèles" d'attaques à rechercher dans les trames capturées. Cette base doit régulièrement être mise à jour.

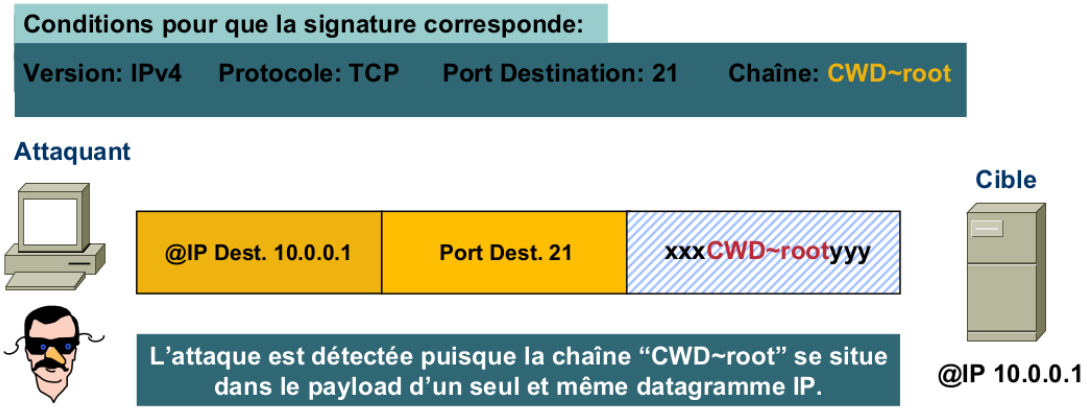
4.2. Analyse par Pattern Matching

Définition

Sur la base des signatures, recherche d'une séquence fixe d'octets contenue dans un seul et même paquet.

Exemple

Attaque basée sur FTP :



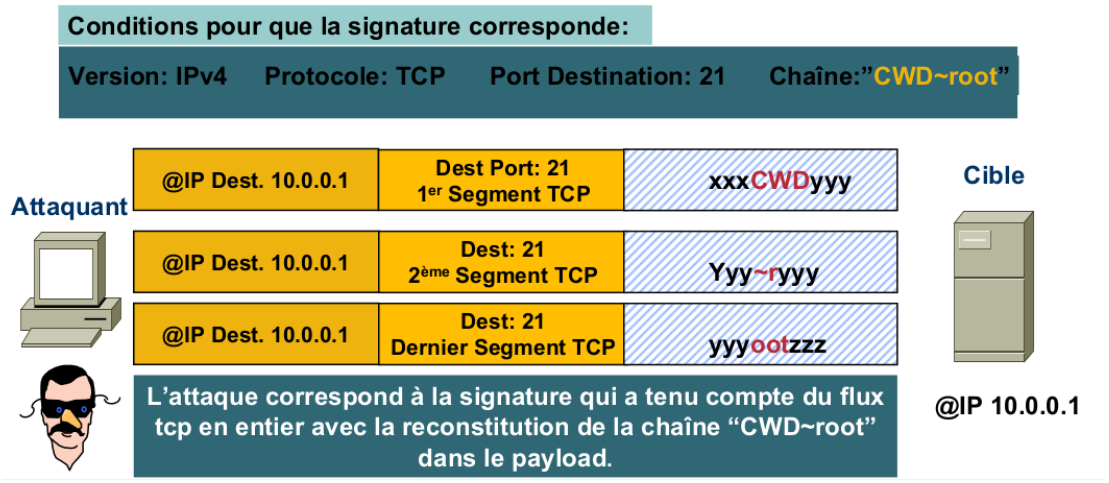
4.3. Analyse par Pattern Matching Statefull

Définition

Sur la base des signatures, considérer l'ensemble des paquets dans un flux TCP. Pour reconstruire la séquence, cela demande de maintenir une table d'état et de rassembler les segments TCP.

Exemple

Signature répartie sur plusieurs paquets :



4.4. Analyse protocolaire

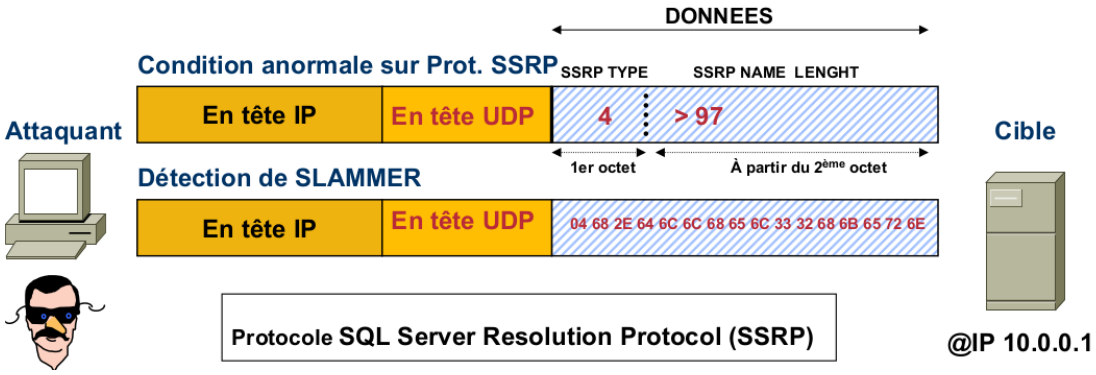
Définition

Analyseur capable de:

- vérifier la conformité du trafic avec la RFC du protocole utilisé
- observer des champs et paramètres suspects pour détecter l'exploitation de valeurs interdites ou l'injection de commandes illicites
- contrôler la longueur de certains champs
- contrôler le nombre d'arguments passés en paramètres

Exemple

Attaque SQL Slammer (*https://fr.wikipedia.org/wiki/SQL_Slammer*) :



4.5. Analyse heuristique

Définition

Repérer des modes de fonctionnement/comportement (et non en utilisant une base de signatures alphanumériques).

Exemple

Règle de détection de scan de port :

> *tentatives successives d'ouverture des ports TCP 1,2,3,4,etc. avec la même IP source et la même IP destination pendant un délai inférieur à 100ms.*

5. Alertes

Lorsqu'un comportement anormal est détecté, différentes actions sont envisageables :

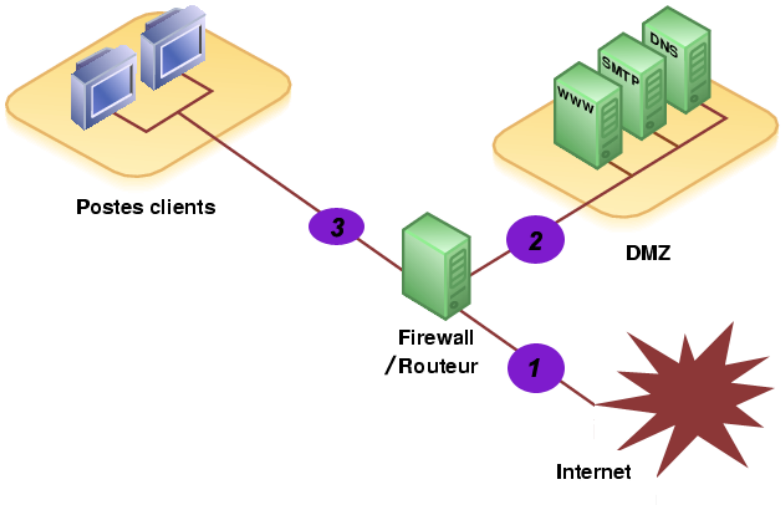
Envoi d'un *trap* SNMP	Envoi de l'alerte (et le détail des informations la constituant) sous format d'un datagramme SNMP à une console de surveillance comme Nagios.
Envoi de messages à un ou plusieurs utilisateurs	Type e-mail ou SMS
Journalisation (log) de l'attaque	Sauvegarde des détails de l'alerte dans une base de données centrale comme par exemple les informations suivantes: *timestamp*, @IP de l'intrus, @IP de la cible, protocole utilisé, *payload*.
Sauvegarde des paquets douteux	Pour analyse ultérieure.

Dans certains cas, l'IDS peut prendre automatiquement certaines mesures :

Reconfiguration d'équipement	Ordre envoyé par le N-IDS à un équipement tiers pour une reconfiguration immédiate dans le but de bloquer un intrus (ACL routeur, règle pare-feu)
Démarrage d'une application	
Fermeture de la connexion TCP	Envoi d'un paquet TCP FIN pour terminer la connexion.

6. Où mettre en place un IDS ?

Le schéma ci-après pose la problématique. Où faut-il mettre l'IDS ? Pas forcément sur le routeur en frontal avec Internet :



1. En amont du firewall, il va détecter l'ensemble des attaques frontales provenant de l'extérieur. Le risque est que beaucoup trop d'alertes soient remontées ce qui les rendra difficilement exploitables.
2. Entre le firewall et la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent donc d'un certain niveau de compétence. Les alertes seront ici plus claires à consulter puisque les attaques bénignes ne seront pas recensées.
3. Entre le firewall et le LAN, il peut ici rendre compte des attaques provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que un grand nombre des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique, ils pourront être identifiés.

TP : IDS

II

Objectifs

Mettre en place l'IDS libre Snort dans pfSense

Installer des règles

Lancer et détecter automatiquement une attaque

On intercale un pfSense entre deux machines. Un scan de port sera lancé depuis une machine attaquante. Ce trafic traversant l'IDS, devra être détecté et signalé.

1. Installation du package IDS

Question

Dans votre pfSense, installer le package "snort"

2. Installation / mise à jour des règles

Question 1

Installez les règles IDS suivantes :

- Snort VRT
- Snort Community

Question 2

Téléchargez et mettez à jour les règles

3. Configuration du pare-feu

Question 1

L'IDS s'ajoute au pare-feu.

Configurer le pare-feu afin d'autoriser les pings entrants : on doit pouvoir pinger la VM derrière le pare-feu.

Question 2

Dans le pare-feu, créer un "alias" permettant de donner un "nom" aux adresses IP du réseau local

4. Préparation de l'IDS

Question 1

Afin d'éviter de fausses alertes, créer une "liste blanche" indiquant quels sont les réseaux IP internes. A faire dans "Services/Snort/Pass lists".

Question 2

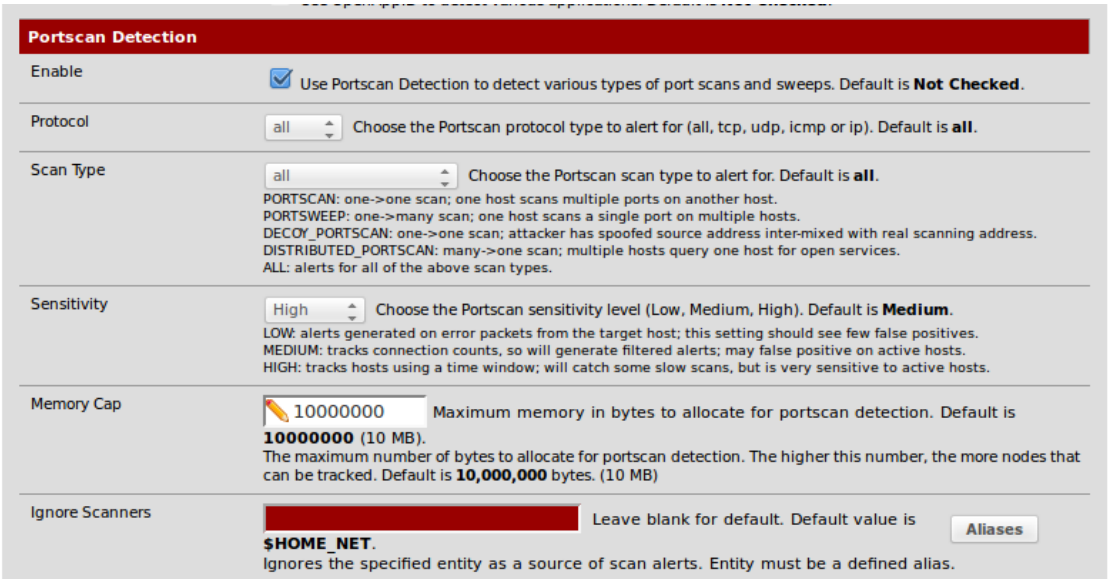
Créer une interface à surveiller dans "Snort Interfaces" affectée au WAN. Mettre le nom de la "pass list" en bas dans "Home Net".

5. Mise en place des règles

Activer les règles :

dans "WAN categories" : choisir "snort_scan.rules"

dans "WAN preprocs" : cocher "Enable" dans "Portscan detection". Mettre "high" dans "Sensitivity".



Dans «Status /Services », démarrer snort.

6. Vérifier le fonctionnement

Lancer une attaque

Maintenant, nous allons valider le fonctionnement de notre snort :

Aller dans « Services / Snort / Alerts », cocher « refresh ».

Avec nmap sous Linux ou zenmap sous Windows, lancer un scan de port vers la VM Windows.

```
# nmap 172.16.0.100

Starting Nmap 6.46 ( http://nmap.org ) at 2015-05-16 09:14 CEST
Nmap scan report for 172.16.0.100
Host is up (0.00097s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds

```

Au bout de quelques instants, on doit voir apparaître dans les alertes :