Configuration et utilisation d'un NIPS/NIDS

Votre responsable vous demande d'approfondir le fonctionnement et la configuration du service NIDS ASQ présent sur les pare-feu UTM Stormshield afin d'améliorer le niveau protection de chaque agence. Votre mission consiste à maîtriser les fondamentaux liés à cet outil puis à implémenter le cahier des charges qui vous a été fourni.

Les outils nécessaires

Les activités suivantes sont à réaliser depuis une VM placée dans le VLAN utilisateur avec les outils suivants (à installer) :

- **nmap** : c'est un logiciel de cartographie de réseaux.

```
$ sudo apt install nmap
```

- **hping3** : c'est un logiciel plus complet que ping qui permet de faire de la cartographie d'un réseau mais également des attaques réseaux (pentesting - test de pénétratio).

```
$ sudo apt install hping3
```

Pour en savoir plmus : https://www.kali-linux.fr/conseil/tuto-hping3-pentesting-reseau

Simulation d'une attaque ayant pour objectif de rendre le service web indisponible

Il est demandé à un administrateur réseau situé sur le VLAN utilisateur d'utiliser les 3 commandes suivantes à destination du serveur web situé en DMZ afin de tester l'efficacité du NIPS/NIDS présent sur le pare-feu :

```
acox@kali:~$ nmap -sS 192.168.228.11
acox@kali:~$ nmap -sU 192.168.228.11
acox@kali:~$ nmap -sV 192.168.228.11
```

- 1. À l'aide d'une capture de trames réalisée depuis la machine attaquante, définir le type de chaque attaque réalisée ainsi que la finalité de chacune de ces commandes.
- 2. Le NIPS a-t-il été en mesure de détecter et de bloquer cette opération ? Justifier.

Dans un second temps, il est demandé à l'attaquant de réaliser l'opération suivante de son VLAN « Utilisateurs » vers l'adresse IP externe du pare-feu d'un autre contexte :

```
acox@kali:~$ hping3 --flood -S -p 80 192.168.230.X
```

- 3. À l'aide d'une capture de trames réalisée depuis la machine attaquante, définir le type d'attaque réalisé ainsi que la finalité de la commande.
- 4. Le NIPS a-t-il été en mesure de détecter et de bloquer cette opération ? Votre service web est-il toujours disponible ? Justifier.

Protections applicatives

- 5. Depuis votre réseau interne, interdire les accès aux boutons « J'aime » ainsi que la possibilité de publier un commentaire sur un mur Facebook.
- 6. Interdire toute action concernant la plateforme de jeu Steam, et le VPN FrozenWay provenant de votre réseau d'entreprise et lever une alerte mineure lorsque cela se produit.

Documents

Document 1 : Qu'est-ce qu'un IDS/IPS ?

Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. Un système de prévention des intrusions (IPS) reprend le principe de l'IDS tout en étant capable de bloquer les activités qu'il considère illégitimes.

Il existe deux grandes catégories d'IDS/IPS :

- les HIDS/HIPS (Host Intrusion Detection System) qui sont des outils de sécurité installés sur des hôtes dans le but de détecter des intrusions ou des comportements anormaux sur ces derniers.
- les NIDS/NIPS (Network Intrusion Detection System) qui sont des équipements ou des services à l'écoute sur le réseau destinés à repérer des flux suspects. Les pare-feu UTM Stormshield sont dotés d'un NIDS/NIPS nommé ASQ (Active Security Qualification).

Ce service repose sur 3 phases :

1. La capture.
2. L'analyse à partir d'une base de signatures, des RFC , de règles applicatives.
3. Les alertes et le blocage potentiel.

La pertinence du placement d'un système NIDS/NIPS sur un réseau est fondamentale, car il doit capturer un maximum de trafic réseau à des fins d'analyse. Plusieurs architectures existent et peuvent être pertinentes. Chacune a ses avantages et ses inconvénients :

- L'IDS/IPS est placé sur le ou les pare-feu de l'entreprise. Les pare-feu sont souvent des équipements pertinents, car ce sont eux qui autorisent ou bloquent la transmission de flux entre les réseaux.
- L'IDS/IPS peut se placer de manière transparente en mode pont sur l'interconnexion principale entre des réseaux afin de jouer son rôle de façon efficace. Les pare-feu Stormshield peuvent d'ailleurs être utilisés à cette fin.
- L'IDS/IPS est connecté sur un port du commutateur en miroir et récupère ainsi les flux émanant des autres ports.

Voici un exemple de schéma décrivant une topologie pour déployer un NIDS/NIPS.

Sur les pare-feu Stormshield, le NIPS est activé par défaut. Cela renforce donc naturellement la sécurité car même en cas d'autorisation globale dans la table de filtrage de l'équipement, ce dernier inspecte et bloque les flux qu'il juge potentiellement dangereux. Bien évidemment, ce service peut générer des faux positifs. Dans le cadre d'un NIPS, les faux positifs sont des flux légitimes que le boîtier a bloqué estimant qu'ils étaient suspects. Avec le temps, l'outil est capable de s'améliorer et de minimiser les faux positifs.

Ce dernier est donc extrêmement complémentaire des autres solutions de sécurité mises en œuvre dans l'entreprise. Sur les pare-feu SNS, il est primordial, sauf cas particuliers, de le laisser activé. Dans le cas contraire, il est possible de basculer en mode IDS ou en mode pare-feu simple (c'est-à-dire filtrage couches 3 et 4).

From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/reseau/stormshield/activitenips

Last update: **2023/12/07 13:22**