MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET UNIVERSITAIRE

UNIVERSITÉ PROTESTANTE AU CONGO

Faculté des sciences informatiques

Sujet : Etude des différents IDPS

Promotion : L2 FASI

Département : Sécurité informatique

Réalisé Par :

MBUYI KASONGA Junior

TUNUNGINI N'LEMVO Exaucée

KHASINDU KISANGULE Bérénice

2023-2024

1. C’est quoi un IDPS ?

Un IDPS (Intrusion Detection and Prevention System) est un système de détection et de prévention des intrusions. Il s'agit d'un dispositif de sécurité utilisé pour surveiller les réseaux, les systèmes informatiques ou les hôtes individuels afin de détecter et de prévenir les activités malveillantes ou les tentatives d'intrusion.

L'objectif principal d'un IDPS est d'identifier les comportements ou les événements suspects qui pourraient indiquer une activité non autorisée ou une violation de la sécurité. Il utilise une combinaison de méthodes de détection, telles que la surveillance du trafic réseau, l'analyse des journaux d'événements, la comparaison de signatures connues de menaces, l'analyse comportementale ou l'utilisation de techniques d'apprentissage automatique.

Lorsqu'un IDPS détecte une activité suspecte, il peut réagir de différentes manières en fonction de sa configuration. Il peut générer des alertes pour informer les administrateurs système, bloquer le trafic malveillant, déclencher des actions de prévention, ou enregistrer les événements pour une analyse ultérieure.

Les IDPS sont utilisés pour renforcer la sécurité des réseaux et des systèmes informatiques en détectant les attaques, les intrusions, les malwares, les tentatives d'exploitation de vulnérabilités et d'autres activités malveillantes. Ils jouent un rôle essentiel dans la défense en profondeur des infrastructures informatiques en complément d'autres dispositifs de sécurité tels que les pare-feu, les antivirus et les systèmes de prévention des intrusions.

2. IDPS basé sur le réseau sans fil

2.1 Principe de détection des IDPS basés sur le réseau sans fil :

1. Surveillance du trafic sans fil : Les IDPS basés sur le réseau sans fil surveillent le trafic des réseaux sans fil, tels que les réseaux Wi-Fi, pour détecter les activités suspectes ou malveillantes.

2. Analyse des protocoles : Les IDPS analysent les protocoles de communication sans fil pour détecter les anomalies ou les comportements non conformes, tels que des tentatives d'authentification non autorisées, des attaques de déni de service ou des tentatives d'intrusion.

3. Détection d'intrusion : Les IDPS basés sur le réseau sans fil utilisent des techniques de détection d'intrusion pour identifier les activités malveillantes, telles que l'utilisation de clés de chiffrement faibles, les attaques par rejeu ou les tentatives d'accès non autorisées.

4. Réponse aux incidents : Lorsqu'une activité suspecte est détectée, l'IDPS peut déclencher des alertes, bloquer l'accès au réseau, limiter les privilèges ou déclencher d'autres actions de prévention.

2.2 Méthodes de détection des IDPS basés sur le réseau sans fil :

1. Détection des anomalies de trafic : Les IDPS analysent les schémas de trafic sans fil pour détecter les variations anormales, les pics de trafic ou les comportements inhabituels qui pourraient indiquer des attaques ou des intrusions.

2. Surveillance des vulnérabilités : Les IDPS basés sur le réseau sans fil surveillent les vulnérabilités connues des protocoles sans fil pour détecter les tentatives d'exploitation ou les attaques ciblées.

3. Détection des attaques d'authentification : Les IDPS analysent les tentatives d'authentification pour détecter les attaques par force brute, les usurpations d'identité ou les tentatives d'accès non autorisées.

4. Analyse des journaux : Les IDPS collectent et analysent les journaux d'événements des équipements sans fil pour détecter les activités suspectes ou les erreurs de configuration.

2.3 Logiciels utilisés pour les IDPS basés sur le réseau sans fil :

1. Cisco Wireless IPS : Solution d'IDPS de Cisco spécifiquement conçue pour les réseaux sans fil, offrant une détection d'intrusion et une protection contre les attaques ciblant les environnements sans fil.

2. Aruba Networks Wireless Intrusion Protection System : Solution d'IDPS pour les réseaux sans fil proposée par Aruba Networks, fournissant une détection et une prévention des intrusions dans les environnements sans fil.

3. AirTight Networks SpectraGuard : Solution d'IDPS sans fil qui utilise des techniques avancées pour détecter les menaces et les attaques dans les réseaux sans fil.

2.4 Déploiement des logiciels IDPS basés sur le réseau sans fil :

1. Placement stratégique des capteurs : Les capteurs d'IDPS sans fil doivent être déployés stratégiquement pour surveiller les zones critiques et les points d'accès sans fil.

2. Configuration et calibrage : Les IDPS sans fil doivent être configurés et calibrés en fonction des caractéristiques spécifiques du réseau sans fil et des besoins de l'organisation.

3. Maintenance et mise à jour : Les IDPS sans fil nécessitent une maintenance régulière pour garantir leur efficacité, y compris les mises à jour des signatures de détection et des règles de sécurité.

6. Conclusion

En conclusion, l'étude des différents types d'IDPS (Intrusion Detection and Prevention Systems) nous permet de constater l'importance croissante de ces systèmes dans la protection des réseaux informatiques contre les intrusions et les attaques malveillantes.

7. Webographie

1. Wikipedia - Intrusion Detection System (IDS):

   - Lien : https://en.wikipedia.org/wiki/Intrusion_detection_system

2. Darktrace:

   - Lien : https://www.darktrace.com/

3. Cisco Wireless IPS:

   - Lien : https://www.cisco.com/c/en/us/products/security/wireless-intrusion-preventionsystem/index.html

4. Aruba Networks Wireless Intrusion Protection System:

   - Lien : https://www.arubanetworks.com/solutions/it-security/wireless-intrusion-protection/