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

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

2.1 Principe de détection des IDPS basés sur le réseau :

1. Collecte de données : Les IDPS basés sur le réseau collectent les données du trafic réseau en utilisant des méthodes telles que la capture de paquets ou l'écoute de flux de données.

2. Analyse du trafic : Les données collectées sont analysées pour détecter des comportements ou des schémas anormaux en utilisant des techniques telles que la comparaison de signatures, l'analyse comportementale et l'apprentissage automatique.

3. Détection d'intrusion : Les données du trafic sont comparées à une base de données de signatures connues de menaces pour détecter les intrusions ou les activités suspectes.

4. Réponse aux incidents : Lorsqu'une intrusion ou une activité suspecte est détectée, des mesures peuvent être prises, telles que l'enregistrement des événements, le blocage du trafic malveillant, la génération d'alertes ou le déclenchement d'actions de prévention.

2.2 Méthodes de détection des IDPS basés sur le réseau :

1. Détection basée sur des signatures : Les IDPS utilisent des signatures préétablies pour détecter des motifs spécifiques correspondant à des attaques connues.

2. Analyse comportementale : Les IDPS surveillent les modèles de comportement du trafic réseau pour détecter les activités anormales ou inhabituelles.

3. Détection d'anomalies : Les IDPS utilisent des modèles de trafic normal pour identifier les écarts significatifs ou les anomalies qui pourraient indiquer des activités suspectes.

2.3 Logiciels utilisés pour les IDPS basés sur le réseau :

1. Snort : Logiciel IDPS open source utilisant des règles basées sur des signatures.

2. Suricata : Logiciel IDPS open source offrant une détection d'intrusion basée sur des règles et une analyse de trafic en temps réel.

3. Bro (Zeek) : Logiciel de surveillance réseau puissant pouvant être utilisé comme IDPS basé sur le réseau.

2.4 Déploiement des logiciels IDPS basés sur le réseau :

1. Placement stratégique : Les IDPS sont déployés dans des positions stratégiques du réseau, tels que des pare-feu, des passerelles ou des points de surveillance du trafic.

2. Mode de déploiement : Les IDPS peuvent être déployés en mode inline, où le trafic passe par l'IDPS avant d'atteindre sa destination, ou en mode passif, où le trafic est copié et analysé sans perturber le flux normal.

3. Configuration et maintenance : L'implémentation des IDPS nécessite une configuration et une maintenance appropriées, y compris la mise à jour des règles de détection, la surveillance des faux positifs, l'analyse des journaux d'événements et la coordination avec d'autres systèmes de sécurité.

3. IDPS basé sur l'Hot

3.1 Principe de détection des IDPS basés sur l'hôte :

1. Collecte de données : Les IDPS basés sur l'hôte collectent des données à partir de l'hôte lui-même, telles que les journaux d'événements, les fichiers système, les modifications de registre et les activités des processus.

2. Analyse des activités : Les données collectées sont analysées pour détecter des schémas ou des comportements anormaux. Cela peut inclure la recherche de signatures de malwares connus, la détection de modifications suspectes de fichiers système, la détection de tentatives d'exploitation de vulnérabilités ou l'analyse comportementale des processus.

3. Détection d'intrusion : Les données collectées sont comparées à des modèles ou des règles de détection pour identifier les activités malveillantes ou suspectes. Cela peut inclure la comparaison avec des signatures de malwares, des règles de détection basées sur des comportements ou des modèles préétablis.

4. Réponse aux incidents : Lorsqu'une activité malveillante ou suspecte est détectée, l'IDPS peut déclencher des alertes, bloquer l'activité, isoler l'hôte du réseau ou déclencher d'autres actions de prévention.

3.2 Méthodes de détection des IDPS basés sur l'hôte :

1. Détection basée sur des signatures : Les IDPS utilisent des signatures préétablies pour détecter des motifs spécifiques correspondant à des attaques connues.

2. Analyse comportementale : Les IDPS surveillent les modèles de comportement des activités sur l'hôte pour détecter les comportements anormaux ou inhabituels.

3. Détection d'anomalies : Les IDPS utilisent des modèles de comportement ou des seuils prédéfinis pour identifier les écarts significatifs ou les anomalies qui pourraient indiquer des activités suspectes.

3.3 Logiciels utilisés pour les IDPS basés sur l'hôte :

1. OSSEC : Logiciel IDPS open source offrant une détection d'intrusion basée sur des journaux d'événements, des fichiers système et des activités des processus.

2. Tripwire : Logiciel IDPS utilisé pour la détection d'intrusion basée sur l'intégrité des fichiers. Il surveille les modifications des fichiers système pour détecter les altérations non autorisées.

3. McAfee Host Intrusion Prevention System : Solution commerciale fournissant une détection d'intrusion basée sur des règles et des comportements sur les hôtes.

3.4 Déploiement des logiciels IDPS basés sur l'hôte :

1. Installation sur chaque hôte : Les logiciels IDPS sont installés et configurés individuellement sur chaque hôte à protéger.

2. Configuration et gestion : Les IDPS basés sur l'hôte nécessitent une configuration et une maintenance appropriées, y compris la mise à jour des règles de détection, la surveillance des faux positifs et la gestion des journaux d'événements.

4. IDPS basé sur l'analyse du comportement du reseau

4.1 Principe de détection des IDPS basés sur l'analyse du comportement du réseau :

1. Collecte de données : Les IDPS basés sur l'analyse du comportement du réseau collectent des données sur le trafic réseau, les flux de données et les activités des utilisateurs.

2. Analyse du comportement : Les données collectées sont analysées pour détecter des modèles, des tendances ou des comportements anormaux qui pourraient indiquer des activités malveillantes.

3. Profilage du comportement : Les IDPS établissent des profils de comportement normal du réseau en surveillant les activités régulières et en identifiant les déviations significatives par rapport à ces profils.

4. Détection d'anomalies : Les IDPS basés sur l'analyse du comportement du réseau utilisent des algorithmes et des techniques d'apprentissage automatique pour détecter les anomalies et les comportements atypiques qui pourraient indiquer des attaques ou des intrusions.

5. Réponse aux incidents : Lorsqu'une activité anormale est détectée, l'IDPS peut générer des alertes, bloquer le trafic suspect, isoler des segments de réseau ou déclencher des actions de prévention.

4.2 Méthodes de détection des IDPS basés sur l'analyse du comportement du réseau :

1. Analyse statistique : Les IDPS utilisent des techniques statistiques pour détecter les modèles et les comportements anormaux, tels que les variations de trafic, les pics d'activité ou les schémas de communication inhabituels.

2. Modèles d'apprentissage automatique : Les IDPS utilisent des algorithmes d'apprentissage automatique pour analyser les données du réseau, identifier les modèles de comportement normal et détecter les écarts significatifs par rapport à ces modèles.

3. Analyse de corrélation : Les IDPS analysent les relations entre différentes activités du réseau pour détecter les schémas d'attaque complexes ou les séquences d'événements anormaux.

4.3 Logiciels utilisés pour les IDPS basés sur l'analyse du comportement du réseau :

1. Darktrace : Plateforme d'IDPS basée sur l'intelligence artificielle qui utilise l'apprentissage automatique pour détecter les anomalies et les menaces émergentes dans le réseau.

2. Vectra AI : Solution d'IDPS basée sur l'analyse comportementale qui utilise l'apprentissage automatique pour détecter les attaques avancées et les menaces internes.

3. Cisco Stealthwatch : Solution d'IDPS basée sur le comportement du réseau qui utilise des analyses avancées pour détecter les activités suspectes et les menaces persistantes.

4.4 Déploiement des logiciels IDPS basés sur l'analyse du comportement du réseau :

1. Placement stratégique : Les IDPS doivent être déployés de manière stratégique sur les segments de réseau critiques pour surveiller le trafic et les activités des utilisateurs.

2. Configuration et calibrage : Les IDPS basés sur l'analyse du comportement du réseau doivent être configurés et calibrés en fonction des caractéristiques spécifiques du réseau et des comportements attendus.

3. Maintenance et mise à jour : Les IDPS nécessitent une maintenance régulière pour s'assurer que les profils de comportement sont à jour et que les algorithmes de détection sont efficaces.

5. IDPS basé sur le réseau sans fil

5.1 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.

5.2 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.

5.3 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.

5.4 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-prevention-system/index.html

4. Aruba Networks Wireless Intrusion Protection System:

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