入侵偵測與防禦系統 (IDS/IPS)

目錄

入侵偵測系統IDS介紹

1. 主要用於偵測是否有非法入侵者入侵，若有非法入侵則向安全管理員發送警告，請求援助。
2. IDS通常放置在防火牆和路由器之間，或DMZ區段及內部網路通往外部網路的咽喉點。
3. IDS分為五種偵測類型：基於網路、基於主機、通訊協定、應用程式通訊協定、混合式，而其中基於網路及基於主機是最為常見的。
4. 透過數據收集和特徵識別技術，系統能夠偵測出與正常活動的偏差，識別出攻擊特徵碼。隨後，分析這些結果並發出警告，確保安全管理員能夠及時應對潛在威脅。

入侵防禦系統IPS介紹

1. 主要是保護主機, 防禦外部及內部的破壞者。
2. IPS通常放置在防火牆和路由器之間, 內嵌在裡面網路架構裡面。
3. IPS分為以下幾種入侵預防類型:基於網路入侵、基於主機入侵、網路行為分析、無線入侵, 而其中基於網路入侵及基於主機入侵是最為常見的。
4. 主要透過流量監控再進行特徵識別識別病毒的特徵碼, 評估及帶來的威脅並採取防禦, 同時放出警報給安全管理員。特徵值的識別對IPS特別重要。

入侵偵測系統IDS 優點及缺點

優點:

1.可以與其他安全防護裝置一起使用 ，如:IPS、防火牆。

2.可以偵測到外部及內部網路的攻擊。

3.詳細記錄所有可疑活動和入侵嘗試, 便於後續分析和調查。

4.相對IPS成本較低。

缺點:

1.現今的網路速度, 所造成傳輸的負擔, 導致效率大打折扣。

2.駭客技術的進步, 通過偵測的機率提升。

3.須定時更新及維護, 以應對不斷變化的安全威脅。

4.需人工進行防禦。

5.管理負擔較重, 容易誤報、漏報。

入侵偵測系統IPS 優點及缺點

優點:

1.可以與其他安全防護裝置一起使用 ，如: IDS、防火牆。

2.可以自動對攻擊方進行反擊及預防, 讓 攻擊方無法達到目的, 使損失降低。

3.夠即時監控和控制進出網絡的流量, 迅速阻斷攻擊行為, 避免進一步的損害。

4.通過先進的特徵識別技術, 可以有效識別和阻止複雜的攻擊模式。

缺點:

1.在進行深度包檢查和行為分析時, 可能會產生誤報或漏報,

2.配置和定期維護成本高

3.須隨時更新軟體, 應對不斷變化的安全脅。

4.現今的網路速度, 所造成傳輸的延遲和瓶頸。

挑戰及發展

現今網路進步飛速, 隨之而來的是許多挑戰:

1.網路傳輸的效率提高, 需分析及偵測的資料也變多, 相對地偵測速度也應提高, 以確保能及時的偵測到危險。

2.加密技術幫系統所增加的複雜性和計算性。

3.駭客技術的進步, 需不斷增IDS/IPS所需技術及防禦能力抵抗。

4.試結合人工智慧技術, 減少誤報和漏報, 提升偵測的準確性和效率。

總結

隨著網路發展越來越普及，網路安全技術也越發的重要，使用IDS、IPS以及其他的安全裝置可以更有效的保護網路安全。

IDS和IPS的主要功能是通過流量監控、特徵識別和威脅評估來保護網絡和系統免受內外部的威脅。IDS 主要負責偵測可疑活動並發出警報，而 IPS 則在偵測到威脅時主動採取防禦措施。

IDS和IPS是保護現代網絡環境的重要工具。通過有效的監控和主動防禦，它們能幫助組織及時發現並應對各種安全威脅。隨著技術的進步和威脅形勢的變化，IDS和IPS 的作用將越來越重要，是構建安全網絡環境的基礎。

參考資料

https://www.paloaltonetworks.tw/cyberpedia/what-is-an-intrusion-prevention-system-ips

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=83

https://www.cc.ntu.edu.tw/chinese/epaper/0054/20200920_5406.html

https://zh.wikipedia.org/zh-tw/%E5%85%A5%E4%BE%B5%E9%A2%84%E9%98%B2%E7%B3%BB%E7%BB%9F