СИСТЕМИ ВИЯВЛЕННЯ АТАК

Хая А.О., В'юхін Д.О., Смірнов А.О.
Харківський національний університет радіоелектроніки Харків, Україна

Метою доповіді є розгляд систем виявлення атак IDS (Intrusion Detection System). Це технологія, що виявляє неправомірні або шкідливі активності в комп'ютерних системах чи мережах [1]. Її основна мета - моніторинг загроз і сповіщення адміністратора про потенційні ризики. IDS може бути програмним забезпеченням або апаратним пристроєм, інтегрованим у систему чи мережу, а дані про підозрілу активність зазвичай передаються адміністратору або системам управління інформацією та подіями (SIEM).

Одним із найпоширеніших методів розвідки перед здійсненням атаки є сканування портів. Це техніка, яку використовують зловмисники для виявлення відкритих портів і доступних сервісів на цільовій системі.

Система IDS, розгорнута в мережі, аналізує трафік і може виявити ознаки сканування портів на основі таких факторів [2]:

– незвичайно висока кількість підключень до різних портів від одного джерела за короткий час;

– наявність специфічних шаблонів запитів, характерних для сканування (наприклад, послідовне надсилання SYN-пакетів без завершення з'єднання);

– використання нестандартних комбінацій прапорців TCP (наприклад, FIN- або XMAS-сканування, що використовується для обходу фільтрації).

Якщо IDS виявляє подібну активність, вона може діяти кількома способами. По-перше, система може вести логування та надсилати сповіщення адміністратору безпеки, що дозволяє оперативно реагувати та блокувати потенційного зловмисника. По-друге, якщо використовується інтегрована система виявлення та запобігання вторгнень (IPS), вона може автоматично блокувати IP-адресу атакуючого через брандмауер або інші засоби захисту. Також IDS може ініціювати зміну параметрів безпеки, наприклад, додавання нових правил у файрвол або обмеження доступу для підозрілих IP-адрес.

Система IDS дозволяє адміністраторам своєчасно реагувати на потенційні загрози. У разі використання інтегрованої IPS, можливе автоматичне блокування атакуючого, що значно знижує ризик подальшого проникнення [3]. Однак для підвищення рівня безпеки важливо також використовувати файрволи, обмеження доступу та оновлення політик безпеки, щоб запобігти несанкціонованому доступу до критично важливих сервісів.

Список літератури

1. Сєвєрінов, О.В., Хрєнов А.Г.. Аналіз сучасних систем виявлення вторгнень. *Системи обробки інформації* 6 (2014): 122-124.

2. Cyberset. IDS (Intrusion Detection System): Захист. 2024. URL: https://cyberset.com.ua/network/what-is-ids-intrusion-detection-system-zakhyst/

3. Barracuda. Intrusion Detection System. URL: https://www.barracuda.com/support/glossary/intrusion-detection-system