

**АВТОМАТИЗАЦІЯ АНАЛІЗУ LOG-ФАЙЛІВ****AUTOMATION OF LOG-FILES ANALYSIS**

IDS (Intrusion Detection System) – це програмні або апаратні системи, які автоматизують процес перегляду подій, що виникають у комп'ютерній системі чи мережі, аналізують їх з точки зору безпеки. Так як кількість мережових атак зростає, IDS стають необхідним елементом інфраструктури безпеки. Аналітику кібербезпеки важливо не лише мати цей інструмент в своєму арсеналі, а й розуміти, для яких цілей призначені IDS, як вибрати та налаштувати IDS для конкретних систем і мережових оточень, як обробляти результати роботи IDS і як інтегрувати IDS з іншою інфраструктурою безпеки підприємства.

Виявлення проникнення є процесом моніторингу подій, що відбуваються в комп'ютерній системі або мережі. Проникнення визначаються як спроби компрометації конфіденційності, цілісності, доступності або обходу механізмів безпеки комп'ютера або мережі. Проникнення можуть здійснюватися як зловмисниками, які отримують доступ до систем з Інтернету, так і авторизованими користувачами систем, що намагаються отримати додаткові привілеї, яких у них немає. Усі події, які відбуваються на персональному комп'ютері (ПК), записуються в спеціальні log-файли, їх ще називають системними файлами, тому що вони містять інформацію про події, які відносяться до програмного забезпечення (ПЗ), безпеки, системи, налаштувань системи, а також час надходження події, її власний ідентифікаційний код та назву виконуваної програми.

IDS володіють функціоналом автоматичного перегляду подій, однак вони, зазвичай, працюють повільно, потребують постійного оновлення даних, не надають детальних даних про події, які виникають в системі, є дуже ресурсо-затратними. Ще однією проблемою є визначення всіх необхідних показників, які можуть бути цінними з точки зору інформаційної безпеки, тому розробка системи, яка може самостійно збирати, систематизувати та аналізувати події на предмет виявлення аномальної поведінки користувача або аномальної мережової активності є актуальним науковим завданням. [1]

Виявлення проникнення завдяки розпізнаванню аномальної поведінки користувачів чи мережі дозволяє організаціям захищати свої системи від загроз, які пов'язані зі зростанням мережової активності, запуском підозрілих процесів, великої кількості невдалих авторизацій, відвідуванням фішингових сайтів. В подальшому дослідженні було розроблено систему, яка здатна самостійно опрацьовувати всі події та фільтрувати їх відносно їх пріоритетності та важливості в цілях попередження про загрозу інформаційній безпеці в ОС (операційних системах) Window та Unix-подібних системах.

Проте не варто вважати, що використання IDS та автоматизація аналізу log-файлів дозволить виявити всі загрози безпеки. Кожен засіб захисту адресовано конкретній загрозі безпеки в системі. Більше того, кожен засіб захисту має слабкі та сильні сторони. Тільки правильно підібравши та налаштувавши ці засоби, можна захиститися від максимально великого спектру атак. [2]

**Література.**

1. What is a Intrusion Detection System. URL: <https://www.barracuda.com/glossary/intrusion-detection-system>. Last accessed: 27.11.2021
2. IDS usability. URL: [https://www.researchgate.net/publication/272476428\\_CASI\\_METHOD\\_FOR\\_IMPROVING\\_THE\\_USABILITY\\_OF\\_IDS](https://www.researchgate.net/publication/272476428_CASI_METHOD_FOR_IMPROVING_THE_USABILITY_OF_IDS). Last accessed: 27.11.2021