Аналіз сучасних програмних та програмно-апаратних засобів виявлення вторгнень

УДК 004.056.53(045)

Анна Корченко[1], Євгенія Іванченко[2], Назим Жумангалієва[3]

[1,2]Національний авіаційний університет, [1]annakor@ukr.net, [2]evivancenko@gmail.com
[4]Казахський національний дослідницький технічний університет ім. К.І. Сатпаєва, [4]nazym_k.81@mail.ru

Інтенсивний розвиток інформаційних систем (ІС) та технологій всебічно впливає на всі сфери діяльності суспільства. Переважна кількість сучасних державних та приватних підприємств використовує ІС для управління виробничими процесами, підтримки прийняття рішень, пошуку необхідних даних тощо. Це забезпечує їм низку переваг, пов'язаних з: підвищенням продуктивності праці і мобільності працівників; високою оперативністю доступу до інформації та послуг; можливостями віддаленого управління ресурсами і процесами тощо.

Разом з цим збільшується кількість уразливостей та загроз ІС і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки.

Слід зазначити, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в ІС з боку неавторизованої сторони. Також слід наголосити, що атаки на ресурси ІС (РІС) з кожним роком стають все досконалішими, глобальнішими та частішими.

Наприклад, низка нещодавно реалізованих кібератак, які завдали шкоди багатьом державним установам та приватним підприємствам і організаціям (Укрпошта, Укрзалізниця, Укренерго, ДТЕК, Київенерго, Київводоканал, Київстар, Lifecell, тощо) показали неготовність та недосконалість їх власних систем безпеки до раніше невідомих вторгнень.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережевих вторгнень використовуються сучасні методи, моделі, засоби, програмне забезпечення (ПЗ) і комплексні технічні рішення для систем виявлення та запобігання вторгнень, які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому, системи виявлення вторгнень (СВВ) повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

Серед таких систем є спеціалізовані програмні засоби, які направлені на виявлення підозрілої активності або втручання в ІС і прийняття адекватних заходів щодо запобігання кібератакам. Ці системи та засоби, як правило,

достатньо дорогі, мають закритий код та вимагають періодичної підтримки розробників (висококваліфікованих фахівців) щодо їх удосконалення і відповідного налаштування до умов конкретних організацій.

Виходячи з цього, проведення аналізу технічних рішень, спеціальних засобів та ПЗ виявлення кібератак, зловживань та аномалій в ІС для їх використання при виборі і розробці СВВ, а також визначення найбільш ефективних відповідних механізмів захисту РІС є актуальним завданням.

Результати аналізу сучасних СВВ та програмних і програмно-апаратних засобів виявлення вторгнень відповідно до базових характеристик «Клас кібератак», «Адаптивність», «Відкритість», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка ОС» інтегровано в таблицю 1. При цьому, розглядались можливості систем щодо реалізації методів виявлення, як-от експертний, статистичний, сигнатурний, графи сценаріїв, контроль зміни подій, кластерний, динамічний, машинного навчання, поведінковий, евристичний, нечітких множин.

Також, відповідно до проведеного аналізу можна зазначити, що сучасні СВВ аномального принципу в основному засновані на математичних моделях, що потребують багато часу для отримання статистичних даних, реалізацію процесу навчання (в основному для нейромережевих систем) та здійснення інших складних і довготривалих підготовчих процедур, того ж, в жодній з проаналізованих систем не використовуються методи нечітких множин які показали свою ефективність при вирішенні такого класу задач. Одним з недоліків аномальних СВВ є процес створення відповідного профіля нормального стану системи, а при її модифікації та інших змінах набрана статистика стає неактуальною та неповною.

Більш ефективні у цьому відношенні є експертні підходи, що засновані на використанні знань та досвіду спеціалістів відповідної предметної області. Крім того, побудова відповідних методів, технічних рішень та створення засобів (СВВ, виявлення кібератак та інші), орієнтованих на обробку слабкоструктурованих даних з метою встановлення фактів несанкціонованого доступу до РІС є основою для успішної протидії відповідним кібератакам.

Більшість СВВ достатньо дорогі, мають закритий код, потребують кваліфікованого налаштування (під певні вимоги організації та сервіси), яке можуть здійснити тільки відповідні спеціалісти. Такі системи переважно не орієнтовані на виявлення раніше невідомих кібератак (0-day атак), а їх спроможність реалізувати задекларовану можливість, теоретично не обґрунтована і не розкривається сам механізм виявлення таких кібератак.

Тому, для таких систем необхідний обґрунтований математичний апарат, наприклад, з використанням теорії нечітких множим, який би дав можливість вирішити проблему виявлення нових типів кібератак.

Практика показує, що на сьогодні існуючі засоби не є ефективними проти нових типів вторгнень. Тому, розробка відповідних методів ідентифікації аномальних станів для СВВ з метою розширення їх функціональних можливостей за рахунок засобів, що використовують відповідний математичний апарат (наприклад, нечітких множим), дасть можливість цим

системам бути дієвими щодо виявлення нових типів кібератак (у тому числі й 0-day атак), які характеризуються невстановленими або нечітко визначеними критеріями у відповідному гетерогенному середовищі.

Таблиця 1

Зведені дані результатів аналізу СВВ

№	СВВ	Класи кібератак				Методи виявлення												Управління системою			Рівень спостереження				Підтримка ОС			
		Зловживання	Аномалії	Адаптивність	Відкритість	Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Централізоване	Розподілене	Масштабованість	Системний	Мережевий	Реакція на кібератаку	Захищеність	Unix	Linux	Windows	MacOS
1	AAFID	+	+	-	+	+	-	+	-	-	-	-	-	-	-	-	+	-	+	+	-	-	-	+	+	-	-
2	Snort	+	+	-	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	+	+	+	+	-
3	Prelude SIEM	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	+	+	+	-	-
4	NetSTAT	+	+	+	+	-	-	+	-	+	-	-	-	-	-	-	-	+	+	+	+	+	+	+	+	-	-
5	Shadow	+	+	-	-	-	-	-	-	+	-	-	-	-	-	-	-	+	+	-	+	-	+	+	+	-	-
6	ASAX	+	-	-	+	+	-	-	-	-	-	-	-	-	-	-	+	-	+	+	-	-	-	+	+	-	-
7	Bro	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	-	-	-	+	+	-	+	+	-	+
8	OSSEC	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	+	+	+	-	+	+	+	+	+	+
9	Cisco IPS	+	+	+	-	-	+	+	-	-	+	-	-	-	-	-	+	+	+	+	+	+	+	+	+	+	-
10	Arbor Networks Spectrum	+	+	+	-	-	+	+	-	-	-	+	-	-	-	-	+	-	+	+	+	+	-	+	+	+	-
11	InfoWatch ASAP	+	+	+	-	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	+	-	-	+	+	+	+
12	Symantec DeepSight Threat Management System	+	+	+	-	+	+	+	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+
13	IPS	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	+	-	+	+	+	+	+	-	-	+	-
14	Tipping Poing NGIPS	+	+	+	-	-	-	+	-	-	-	+	+	-	-	-	-	+	+	+	+	+	+	-	-	+	+
15	Axoft inv GUARD	+	+	-	-	-	+	+	-	-	-	+	-	+	+	-	+	-	+	+	+	-	-	+	+	-	-
16	Defense Pro	+	+	+	-	-	+	+	-	-	-	-	-	+	-	-	+	-	+	-	+	+	+	+	+	+	+
17	KATA Platform	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	-	+	+	+	+	+	+	+	+	+	+
18	Suricata	+	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	-	+	+	+	+
19	Samhain	+	+	+	+	-	+	-	-	-	-	+	-	+	-	-	+	+	+	+	-	+	+	+	+	+	+
20	Security Onion	+	+	+	+	-	+	+	-	+	-	+	-	+	-	-	+	+	+	+	+	+	-	+	+	-	-

Такі розширені можливості СВВ дозволять їм, фактично, залишатися функціональними у потенційно небезпечному оточенні характерному впливам різноманітних загроз.