УДК 004.056
А. Сюшко; І. Скарга-Бандурова, д. т. н., проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПОБУДОВА СИСТЕМИ МОНІТОРИНГУ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРІЇВ НА ОСНОВІ OSSEC

UDC 004.056
A. Siushko; I. Skarga-Bandurova, Dr., Prof.

BUILDING AN END-DEVICE SECURITY MONITORING SYSTEM BASED ON OSSEC

Швидкий розвиток інформаційних систем є прямопропорційний до розвитку кіберзагроз, таке явище зумовлює потребу у впровадженні ефективних механізмів контролю стану кінцевих пристроїв. Хостові системи виявлення вторгнень (HIDS) посідають важливе місце в архітектурі комплексного захисту, оскільки забезпечують безперервний моніторинг подій, аналіз поведінкових відхилень та контроль цілісності критично важливих компонентів операційної системи. Саме тому дослідження принципів їх функціонування та практичне розгортання конкретних інструментів є актуальною задачею сучасної кібербезпеки.

У рамках роботи проведено системний аналіз принципів функціонування хостових та мережевих систем виявлення вторгнень, здійснено їх порівняльну характеристику та окреслено ключові переваги HIDS у контексті виявлення локальних інцидентів безпеки. На основі класифікації відкритих рішень для моніторингу встановлено, що OSSEC є одним із найбільш збалансованих інструментів, який поєднує розвинений набір функцій, відкритість програмного коду та можливість масштабування у різних типах інфраструктур.

Особливу увагу приділено аналізу методів виявлення вторгнень, зокрема сигнатурному та аномалічному підходам, а також їхній ефективності під час обробки подій, отриманих від кінцевих пристроїв. Розглянуто значення коректного ведення лог-файлів як основи для подальшої кореляції, формування правил детекції та побудови автоматизованих реакцій на інциденти.

Практична частина роботи охоплює процес розгортання сервера OSSEC, початкове конфігурування системи, підключення агенту в середовищі Windows та тестування механізмів реєстрації й аналізу подій. Під час експериментального дослідження проаналізовано ефективність системи в умовах реального моніторингу: виявлення змін у файловій системі, фіксація підозрілої активності та роботу механізмів автоматичного реагування.

Отримані результати підтверджують доцільність використання OSSEC як надійного та функціонального інструмента для побудови системи моніторингу безпеки кінцевих пристроїв. Система забезпечує ефективне виявлення інцидентів, підвищує рівень захищеності інформаційного середовища та може бути рекомендована для використання в організаціях різного масштабу.

Література

1. Sachenko A.O., Kochan V.V., Bykovyy P.Ye., Zahorodnia D.I., Osolinskyy O.R., Skarga-Bandurova I.S., Derkach M.V., Orekhov O.O., Stadnik A.O., Kharchenko V.S., Fesenko H.V. Internet of Things for intelligent transport systems: Practicum / A.O. Sachenko (Eds.) – Ministry of Education and Science of Ukraine, Ternopil National Economic University, Volodymyr Dahl East Ukrainian National University, National Aerospace University “Kharkiv Aviation Institute”, 2019. – 135 p.