СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖІ

Ляшенко О. С., Гольцев Д. О., Мельникова К. С.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком Інтернету протягом останніх декількох років потреба в безпеці зростала внаслідок цього, головним чином, завдяки відкритості та підключеності Інтернету. Люди та організації щодня стикаються з великими труднощами, щоб захистити свої дані та зберегти цінні активи. Запобігання, виявлення та реагування є частиною моделі захисту мереж. Системи виявлення вторгнень є важливими складовими оборонних заходів, що захищають комп'ютерні мережі від зловживань. Система виявлення вторгнень (СВВ) повина виявити зловмисника, що проникає в систему, або законного користувача, який неправильно використовує системні ресурси [1]. Система виявлення вторгнень на основі мережі та система виявлення вторгнень на основі хоста - це дві основні моделі виявлення вторгнень. Мережева система виявлення вторгнень (МСВВ) здійснює моніторинг трафіку на мережевому рівні та намагається виявити, чи хакер/зловмисник намагається вторгнутися в систему чи атакою викликати відмову служби. Система виявлення вторгнень на основі хоста перевіряє дані з одного хоста для виявлення вторгнення. Мережа надає дані в механізм правил і нормалізатор активності. Механізм правил здійснює пошук даних для зразків з відомої бази даних зловмисних дій. Нормалізатор діяльності виконує аналіз даних.

Метою доповіді є аналіз підходів виявлення вторгнень, які використовуються в розглянутій системі. Підходи можна класифікувати: виявлення зловживань та виявлення аномалії. Виявлення зловживання виявляє вторгнення згідно правил регулятора активності датчика та звітує про відому шкідливу активність. Це включає моніторинг мережевого трафіку в пошуку прямих відповідностей відомим моделям атаки. Недоліком такого підходу є те, що він може виявляти лише вторгнення, що відповідають заздалегідь визначеній схемі. Під час виявлення аномалії система заздалегідь визначає очікувану поведінку мережі чи профілю. Будь-які значні відхилення від цієї очікуваної поведінки потім передаються як можливі атаки. В роботі було розроблен інструмент обміну даними, який описує поведінкову експертизу щодо виявлення вторгнень.

Список літератури

1. Ляшенко О.С. Аналіз систем і засобів захисту підприємства / О.С. Ляшенко, Мусаб Нур Еддін Аллахам, О.В. Кісь // Проблеми інформатизації, 7 міжнародна науково-технічна конференція 13-15 листопада 2019 р. – Т.1., С. 52.